Transport Canada
Development

Transports Canada
Développement

TP 5045E

TRANSPORTATION SAFETY
A Framework for R&D Planning

Main Report

Prepared for

Transportation
Development Centre

DECEMBER 1983

Canada

6&5

Canada

TP5045

Library and Information Centre /
Centre de Documentation (GSLA)
RECEIVED – REÇU LE
MAR 21 1984
Transport Canada / Transports Canada

TRANSPORTATION SAFETY:
A Framework for R&D Planning

MAIN REPORT

Prepared by

PEAT, MARWICK AND PARTNERS

for the

TRANSPORTATION DEVELOPMENT CENTRE

December 1983

The contents of this report reflect the views of the contractor and not necessarily the official views or policies of the Transportation Development Centre.

PROJECT TEAM

The project team consisted of:

Mr. M.E. Kieran	- Peat, Marwick and Partners
Mr. R.M. Allingham	- Peat, Marwick and Partners
Mr. J.F. Woods	- Peat, Marwick and Partners

REPORT DOCUMENTATION FORM

1. Transport Canada Report No
TP5045

2. TDC Project No
4557

3. Recipient's Catalogue No

4. Title and Subtitle
Transportation Safety: a Framework for R&D Planning
Main Report

5. Report Date
December 1983

6. Performing Organization Report No

7. Author(s)
M. Kieran
R. Allingham
J. Woods

8. Transport Canada File No
D 1450-126-1

9. Performing Organization Name and Address
Peat, Marwick et Associés
1155 Dorchester Blvd. West, 25th Floor
Montreal, Quebec, H3B 2J9

10. DSS File No
11SD.T8200-2-2539

11. DSS or Transport Canada Contract No
OSD82-00132

12. Sponsoring Agency Name and Address
Transportation Development Centre (TDC)
1000 Sherbrooke St. West
Montreal, Quebec, H3A 2R3

13. Type of Report and Period Covered
Final Nov. 82 - Sept.83

14. Sponsoring Agency Code
TDC 4557

15. Supplementary Notes
Separate summary reports bear the numbers TP5046E (English version) and TP5046F (French version)

16. TDC Project Officer
Barry Myers

17. Abstract

The report describes a system safety methodology, applicable to all transportation systems, to assist in establishing research and development needs and to provide a measure of the safety improvements achievable through R&D and other system changes.

The study provides a detailed review of the state-of-the-art of system safety and other approaches to transportation safety program and R&D planning in the public sector. Mission-orientation and the relationship of R&D planning methods to mission-dependency on R&D and on the ongoing Program structure of public agencies and institutions is stressed. A detailed review is conducted of planning methods introduced into a number of U.S. Department of Transportation Agencies. A method of safety R&D planning is proposed based on work conducted by Battelle Columbus Laboratories for the United States Coast Guard. An attempt is made to demonstrate the potential usefulness of the proposed approach by performing a safety problem analysis in the air mode. It is suggested that the Canadian Air Transportation Administration would be the most appropriate starting point for a pilot implementation of the planning framework proposed.

18. Key Words
Safety - System Safety - Research and Development - Planning - Transportation

19. Distribution Statement
Limited number of copies available from TDC

20. Security Classification (of this report)

21. Security Classification (of this page)

22. No. of Pages
70

23. Price

FORMULE DE DOCUMENTATION POUR RAPPORT

1 **N° du rapport Transports Canada**
TP5045

2 **N° de l'étude — CDT**
4557

3 **N° de catalogue du destinataire**

4 **Titre et sous-titre**
La sécurité des transports: un cadre pour la planification de la recherche et du développement.
Rapport principal

5. **Date du rapport**
Décembre 1983

6. **N° du rapport de l'organisme exécutant**

7. **Auteur(s)**
M. Kieran
R. Allingham
J. Woods

8. **N° de dossier Transports Canada**
D 1450-126-1

9. **Nom et adresse de l'organisme exécutant**
Peat, Marwick et Associés
1155 ouest, boul. Dorchester, 25e étage
Montréal (Québec)
H3B 2J9

10. **N° de dossier — ASC**
11SD.T8200-2-2539

11. **N° de contrat — ASC ou Transports Canada**
OSD82-00132

12. **Nom et adresse de l'organisme parrain**
Centre de développement des transports (CDT)
1000 ouest, rue Sherbrooke
Montréal (Québec)
H3A 2R3

13. **Genre de rapport et période visée**
Final

14. **Code de l'organisme parrain**
TDC 4557

15. **Remarques additionnelles**
Rapports sommaires distincts portent les numéros TP5046E (version anglaise) et TP5046F (version francaise)

16. **Agent de projet — CDT**
Barry Myers

17. **Résumé**

Le rapport décrit des méthodes applicables à tous les systèmes de transport et ayant pour but d'aider à l'identification des besoins en recherche et développement de même qu'à l'évaluation quantitative des améliorations en matière de sécurité, susceptibles d'être apportées grâce à la recherche et au développement et autres changements des systèmes.

L'étude comporte un examen détaillé des techniques les plus modernes en matière de sécurité des systèmes de transport et de planification de la recherche et du développement dans le secteur public. L'accent est surtout mis sur l'orientation des missions et la relation qui existe entre les méthodes de planification de la recherche et du développement et le degré de dépendance des missions de la recherche et du développement et de la structure des programmes en cours des agences et institutions gouvernementales. Un examen détaillé des méthodes de planification introduites dans un certain nombre d'agences du département américain des transports a été effectué. Une méthode de planification de la recherche et du développement en matière de sécurité a été proposée; celle-ci est fondée sur le travail effectué par Battelle Columbus Laboratories pour le compte de la garde-côte américaine. En outre, on tente de démontrer l'utilité possible de la méthode proposée en effectuant une analyse du problème que pose la sécurité dans le domaine du transport aérien. Il semblerait que l'administration canadienne des transports aériens soit le point de départ par excellence pour la mise en application, à titre d'essai, de la structure de planification proposée.

18. **Mots-clés**
Sécurité - Sécurité des systèmes
Recherche et développement -
Planification - Transports

19 **Diffusion**
Nombre limité de copies disponibles au CDT.

20. **Classification de sécurité (de ce rapport)**

21. **Classification de sécurité (de cette page)**

22 **Nombre de pages**
70

23 **Prix**

CDT TDC 79-005

ACKNOWLEDGEMENTS

The authors gratefully acknowledge the assistance provided by the personnel of Transport Canada, including Mr. M. Tapiero, Mr. B. Myers, and Ms. Judith Nogrady of the Transportation Development Centre; and the personnel of U.S. Department of Transportation Agencies, including Dr. John G. Gardinier of the U.S. Coast Guard and Mr. Barry Felrice of the National Highway Traffic Safety Administration.

TABLE OF CONTENTS

Page

1. INTRODUCTION 1
   - 1.1 Background 1
   - 1.2 Concepts, Terms and Definitions 2

2. INSTITUTIONAL DIMENSIONS OF R&D PLANNING 11
   - 2.1 The Concept of Mission Dependency 11
   - 2.2 Implications for Safety R&D Planning in Canada 13
   - 2.3 Transportation Data Sources in Canada 15

3. CONCEPTUAL PROBLEMS OF SAFETY R&D PLANNING 22
   - 3.1 The Measurement of Safety 22
   - 3.2 Perceived and "Statistical" Safety 26
   - 3.3 Levels of "Acceptable" Risk 27
   - 3.4 Program versus Project Planning 27
   - 3.5 Accident Prevention versus Accident Protection 28
   - 3.6 Project Evaluation 28

4. SYSTEMATIC TRANSPORTATION SAFETY PLANNING METHODS 29
   - 4.1 Introduction 29
   - 4.2 The R&D Planning Process 30
   - 4.3 The National Highway Safety Needs Reports of 1976 and 1981 31
   - 4.4 The National Highway Traffic Safety Administration 1983 Safety Priorities Plan 35
   - 4.5 Federal Highways Administration Rational Determination of Priority Targets for Research and Development 39
   - 4.6 Federal Railroad Administration Track Rehabilitation and Maintenance Research Requirements 41
   - 4.7 Urban Mass Transportation Administration Safety Program Plan 44
   - 4.8 U.S. Coast Guard Research, Development Testing and Evaluation Plan 48

Page

5. AN APPROACH TO IDENTIFYING SAFETY R&D NEEDS 57
  5.1 Introduction 57
  5.2 Framework for an Approach to Identifying Transportation Safety R&D Needs 58
  5.3 Approach to Identifying Safety R&D Needs in the Air Mode 63
  5.4 Conclusions from the Demonstration of the Safety R&D Needs Identification Methodology in the Air Mode 69

List of Appendices

A. Results of Fact Finding (Task 1 of Work Program)
B. U.S. Department of Defense Requirements for a System Safety Program
C. System Safety Applications to Transport Safety
D. Compendium of Hazard Analysis Techniques
E. Selected Bibliography

List of Exhibits

Opposite Page

2.1 Management Process for R&D in Government Laboratories 14
3.1 Modal Distribution of Fatalities (Comparison of Canada vs. U.S.A., 1981) 21
4.1 Safety R&D Support of Agency Mission Objectives and Programs 29
4.2 The Role of Problem Identification in the System's Approach to Program Development 32
4.3 Framework for Highway R&D Evaluation 40
4.4 UMTA/OSPQ Program Plan Study. Critical and Specific Objectives for Key Objective No. 1 45
4.5 Hazard Identification and Evaluation Process 45
4.6 UMTA/OSPQ Safety Program Plan Study. Rail Hazard Area Ratings 46
4.7 UMTA/OSPQ Safety Program Plan Study. Rail Rapid Transit. People Exterior to Train. Accident Scenario 47
4.8 UMTA/OSPQ Safety Program Plan Study. Rail Rapid Transit. People Exterior to Train. Accident Countermeasures and Mitigations

List of Exhibits

	List of Exhibits	Opposite Page
4.9	Identification of Parties-at-Risk	51
4.10	Primary Problem Area Logic Diagram	52
4.11	Symbols Used in Logic Diagrams	52
4.12	Logic Diagram for Primary Problem Area 07 - Flooding, Capsizing, Foundering	52
5.1	Logic Diagram Showing Parties-at-Risk and Estimated Safety Problem Seriousness	71
5.2	Logic Diagram Showing Primary Problem Areas for "Aircraft-at-Risk"	72
5.3	Logic Diagram Showing Primary Problem Areas for "Crew/Passengers-at-Risk"	73
5.4	Logic Diagram Showing Primary Problem Areas for "Infrastructure/Facilities-at-Risk	74
5.5	Logic Diagram Showing Primary Problem Areas for "Environment-at-Risk"	75
5.6	Logic Diagram Showing Primary Problem Areas for "Public-at-Risk"	76
5.7	Subproblem Analysis for Primary Problem Area "Collision/Crash in Flight"	77
5.8	Subproblem Analysis for Primary Problem Area "Fire/Explosion in Flight"	78
5.9	Subproblem Analysis for Primary Problem Area "Aircraft Systes Primary Failure"	79
5.10	Subproblem Analysis for Primary Problem Area "Survival Equipment/Procedures LTA"	80
5.11	Subproblem Analysis for Primary Problem Area "Operational Degradation of the Environment"	81

1. INTRODUCTION

1.1 Background

Since 1970, the Transportation Development Centre (TDC) has been a focus for the application of science and technology to improve transportation in Canada. The research and development undertaken by TDC is directed towards one main goal: "the application of R&D results toward the solution of real transportation problems". Transportation safety is numbered among these problems.

In 1980, an assessment of transportation safety issues, priorities and programs within Transport Canada revealed a need for a departmental overview of safety in transportation, particularly in terms of what R&D can contribute to the achievement of safety objectives and how allocations of funds should be made. Safety objectives must often be set without consistent safety information and a mode of reacting to crises was identified.

This called for a more systematic and comprehensive planning approach. TDC, as the appropriate instrument to take the lead in developing an overall approach to the identification of R&D needs in the field of transportation safety, commissioned the present study to develop a systematic methodology to assist in identifying safety R&D needs in the various modes.

1.1.1 Objectives

The present study has the following formal project objective:

"To develop a systems safety methodology applicable to all transportation systems which will assist in establishing research and development needs and provide a measure of the safety improvements achievable through R&D and other system changes."

This process is undertaken in support of the overall Departmental mission goal "to ensure that an adequate level of safety is provided for the national transportation system". It is not intended that such a method would eliminate or substantially modify the existing structures of decision-making. Rather, the method may be used to assist program management by providing the necessary additional information for decision-making.

While the methodology is primarily designed to be used in the context of public sector mission-oriented planning for transportation safety R&D, there should be no intrinsic barrier to its eventual adoption in the private sector.

1.1.2 Study Approach

The methodology development was undertaken on the basis of a heuristic approach which combined exploratory fact-finding and feed-back, which was then used to conduct further exploratory work. The sequence of tasks was as follows:

Task 1: Collect data and information
Task 2: Define methodology

Task 3: Develop modelling framework
Task 4: Demonstrate and test modelling framework

The actual development of the methodology draws heavily on similar work undertaken for the various Agencies of the U.S. Department of Transportation, in particular at the U.S. Coast Guard.

1.1.3 Report Structure

The report is divided into five main sections. Following this introduction, the institutional dimensions of R&D planning in government are outlined. This is considered to be an important determinant to the success or failure of technical methods of identifying R&D needs in government, specifically in Transport Canada. This section is followed by a consideration of some of the conceptual problems that must be solved by any viable methodology. The fourth section reviews the several technical approaches to R&D planning in the United States and Canada. The main focus of the report is section five, which describes the methods used to identify safety problem areas, the development of project areas and the ranking and evaluation of R&D proposals. The final chapter demonstrates the application of the method to the air mode.

The results of the detailed fact-finding work that was conducted in connection with this research effort is given in Appendix A.

1.2 Concepts, Terms and Definitions

The scope and focus of application of the present research effort is governed explicitly by the work program and objectives of study, but also implicitly by the meanings that are attached to the various terms used to describe these objectives and potential areas of application.

Explicitly, the work program itself included the following major areas of work activity:

- a review of transportation safety R&D planning in all modes;

- the development of a stuctured approach to the establishment of transportation safety R&D needs in all modes;

- the application of system safety concepts and techniques to do this, where appropriate; and

- a demonstration of the use of such an approach (in a single mode).

In accordance with the original terms of reference of this study, investigation is restricted to those safety elements related to "vehicles, drivers, occupants or cargo, and their service operations, maintenance and training. Not included are any events which would be considered in the realm of industrial accidents, or are entirely non-travel-related".

Implicitly, the thrust and scope of the work is governed in no small way by the manner in which the various terms in the statement of objectives are understood, particularly such terms as safety, system safety and related terminology.

1.2.1 Safety, "System Safety" and Related Terminology

While the notion of safety might appear quite obvious at first sight, experience has shown that this concept is generally defined in accordance with the philosophical dispositions and practical intentions of the author.

In essence, however, safety may be understand in two ways, as a certain end-state of existence or as something to be done (i.e. a means) to prevent harm to somebody or something. In short it is susceptible of a condition definition or of an activity definition.

The United States Department of Defense* for example, uses a condition definiton to define safety as:

> Safety
>
> "Freedom from those conditions that can cause death, injury, occupational illness, or damage to or loss of equipment or property."

A previous study** by the Transportation Development Agency (TDA) also used a condition definition to define the specific area of transportation safety as follows:

> Transportation Safety
>
> "Transportation safety can be defined as an optimum state where there are no accidents, incidents, and surprises in the transportation process."

However, a follow-up pilot research study by the Intendes Group Limited identified a number of alternative definitions, framed in terms of:

- who is concerned;
- how they are concerned;
- what they expect with regard to safety.

---

* U.S. Department of Defence. Military Standard on System Safety Program Requirements (MIL-STD-882A), Washington, June 28, 1977.

** Ling Suen and S. Bergen Henengouwen. Research Proposal for Transportation Safety. Montreal, Transportation Development Agency, 1970.

This study adopted an activity definition in proposing that:

Safety

"safety is a function of anticipating undesirable consequences of behaviour and the capability to alter these consequences".*

When the word system is combined with safety in the term "system safety", the emphasis tends to focus on both means and ends (the condition of "safety"). The best example is the definition provided by the United States Department of Defense (MIL-STD-882A). System safety is:

System Safety

"The optimum degree of safety within the constraints of operational effectiveness, time, and cost attained through specific application of system safety management and engineering principles whereby hazards are identified and risk minimized throughout all phases of the system life cycle."

The Intendes study correctly pointed out that there can be no right or correct definition of safety which would deny the validity of all others. For a military system for example, the condition of being free of all accidents is a sine qua non of the success of the system. For purposes of identifying "the safety improvements achievable through R&D and other system changes" however, the achievement of absolute (or ideal) safety is impractical and safety must be defined in terms of some socially acceptable level of safety. An activity definition of safety is more appropriate in this context, since it opens the possibility of anticipating the consequences of transportation events and devising interventions (e.g. R&D programs) to reduce the incidence of undesirable consequences (e.g. accidents, incidents and surprises), and to mitigate these consequences when they do occur. We therefore prefer the Intendes approach to defining safety, leaving open for the moment, the task of deciding just what level of safety might be "acceptable".

When it comes to defining system safety, we have no quarrel with the U.S. Military Standard definition in this matter. In developing a system safety methodology to assist in establishing R&D needs we will clearly seek to apply the appropriate system safety management and engineering principles to identify hazards and minimize risk (specifically the risk of transportation accidents). In this connection, we also find it useful to adopt the MIL-STD-882A definitions of a number of other system safety terms that will appear through this report. These include the following:

---

* Intendes Group Ltd. "Pilot Research Study on Transportation Safety". Prepared for the Transportation Development Agency, Transport Canada, March 1972.

System. A composite, at any level of complexity, of operational and support equipment, personnel, hardware, and software procedures which are used together as an entity and capable of performing and/or supporting an operational role.

Accident (Mishap). An unplanned series of events that result in death, injury, occupational illness, or damage to or loss of equipment or property*.

Risk. An expression of a possible loss in terms of hazard severity and hazard probability.

Hazard. An existing or potential condition that can result in an accident.

Hazard Probability. The likelihood, expressed in quantitative or qualitative terms, that a hazard will occur.

Hazard Severity. A qualitative assessment of the worst potential consequence, defined by the degree of injury, occupational illness, property damage, or equipment damage that could ultimately occur.

These various definitions have been used extensively throughout the literature on system safety, and we see no reason for departing from them here.

It must be remembered throughout this study however, that we do not use system safety in the military systems sense of applying system safety management and engineering principles to technical design objectives for safety. Rather we would seek to used certain system safety principles and techniques in the formulation of a method designed to identify areas of R&D need in the context of overall government mission objectives in safety.

1.2.2 Research and development in safety

The thrust and scope of work is also governed by the scope which is given to the notion of research and development. Research and Development is often divided into "soft" areas of socio-economic type R&D and "hard" areas of technology-oriented R&D**. In effect, R&D may be understood in either a narrow or in a very broad sense.

---

* An incident is also an unplanned series of events. It is virtually the same in structure as an accident, the difference being that in an accident, the terminal event results in injury or damage.

** cf. John Heads, "The Organization of Transportation Research in Government to meet the Challenges of the 1980's". Paper presented to the 16th Annual Meeting of the Canadian Transportation Research Forum, Charlottetown, June 10-12, 1981.

Revenue Canada

An example of a narrow (technical) understanding of R&D is the definition used by Revenue Canada in the context of private enterprise. Research and Development is:

> "Systematic investigation carried out in the natural and engineering sciences by means of experiments or analysis to achieve a scientific or commercial advance. Research is original investigation undertaken on a systematic basis to gain new knowledge; development is the application of research findings, or other scientific knowledge, for the creation of new or significantly improved products or processes."

Science Council of Canada

A somewhat broader definition is provided by the Science Council of Canada, reporting on a survey of Canadian Activity in the specific area of transportation R&D in 1971*. Research and development:

> "includes all activities by governments, university and industry which are concerned with increasing our knowledge of transport systems as they are today, what has caused them to be that way, and what might be done to improve them in the future".

U.S. Department of Transportation

The most comprehensive and also detailed definition on research and development applied to the specific field of transportation is probably the one developed by the U.S. Department of Transportation (DOT), who established an in-house Task Force to compare R&D activities at the DOT with those in other U.S. Government Agencies**. Admitting that most definitions of R&D are tailored to fit the type of work conducted within a specific government agency, the study proposed the following distinctions:

---

* C.B. Lewis, A Survey of Canadian Activities in Transportation R&D, Background Study for the Science Council of Canada, May 1971.

** U.S. Dept. of Transportation. Research and Development Activities in the Department of Transportation and Selected Federal Agencies, December 1980. Washington, NTIS PB 81-132888.

"Research is a systematic study directed toward fuller scientific knowledge or understanding of the subject studied.

In Basic Research, the objective of the sponsoring agency is to gain fuller knowledge or understanding of the fundamental aspects of phenomena and of observable facts without specific application toward processes or products in mind.

In Applied Research, the objective of the sponsoring agency is to gain knowledge or understanding necessary for determining the means by which a recognized and specific need may be met.

Development is systematic use of knowledge or understanding gained from research, directed toward the production of useful materials, devices, systems, or methods, including design and development of prototypes and processes. It excludes quality control, routine product testing, and production.

Exploratory Development includes post-research efforts directed to the solution of specific problems short of full development.

Advanced Development includes activities which are aimed at implementation of a specific system or solving a specific problem in an existing system which requires a major effort.

Prototype Development includes the actual construction of a prototype.

Testing and Evaluation are usually grouped together and are performed on prototypes which have resulted from a development process to determine system performance, technical feasibility, practicability, operational performance, and suitability for operational deployment.

Demonstration includes activities associated with providing and supporting an initial system operational capability, the detection of fault and installation problems, the evaluation of user and operator acceptance, and making any improvements required. It includes the integration of the system with the real operating environment, and the evaluation of reliability, maintainability and cost of system operations in such an operational environment."

Transport Canada

The notion that research and development in government is conducted in support of overall departmental mission goals is recognized by Transport Canada who identify three general areas of R&D support. R&D initiatives may be undertaken in support of:

- direct departmental needs - where the prime use is to implement regulations, improve statutory services or introduce new services;

- specific current needs - where the department or the government augments efforts of the other sectors to accelerate progress in transportation areas of pressing national concern;

- general needs - where the department or the government identifies the lack of adequate response of other sectors in a priority transportation area and assumes the responsibility to seek ventures through high risk work to enhance the ventures' viability.

In addition to the primary efforts related to specific system applications or equipment, some work may be directed toward the discovery of fundamental knowledge in order to identify options in support of long-range planning requirements.

The definition of R&D used by Transport Canada is also a comprehensive one (through not as detailed as that used by the U.S. DOT), Research and Development is considered to be:

"Creative work and related activities undertaken on a systematic basis to support Transport Canada's objectives. Creative work comprises one or more of the following elements:

- Basic research - increasing the stock of scientific and technical knowledge;
- Development - discovering new techniques, methods, equipment and systems; or discovering new applications for existing knowledge, techniques, methods, equipment and systems;
- Demonstration - testing and evaluating new techniques, methods, equipment and systems."

Research and development covers the whole of the innovation cycle and may include concept definition and design development of new systems and equipment; feasibility studies, laboratory experimentation detailed design and engineering of prototypes; building, testing, development, demonstration and evaluation of prototype equipment and systems.

Related activities are further defined to include operations research, applied mathematics, collection, analysis and dissemination of program specific state-of-the-art technical data arising out of technical assessment and development, and socio-economic analyses such as program specific market, financial and environmental studies, if related to the planning of R&D activities or to the assessment of the products of R&D activities.

1.2.3 The Scope of Application of the Methodology

While the Transport Canada notion of research and development would appear to encompass all the various activities that might conceivably be undertaken in support of transportation safety programs, including "human factors" as well as technology-based R&D, the scope of application of the methodology is restricted to a specific area, that of transportation safety. This presents a problem in the particular context of Transport Canada (and other government Agencies) since the Department's strategic objective in safety is only one among nine strategic objectives which are met through the various departmental policies and programs. Programs are often multimission in their objectives and e.g. government spending in the interests of transportation safety or transportation safety R&D is often difficult to identify*. A recent study by the Strategic Planning Group** draws attention to this problem by recognizing the tripartite nature of safety within departmental planning and programming as follows:

- Level of safety for facilities/services where safety is an output measure of a transportation activity or a criteria by which the system is assessed based on an objective of operational efficiency. A level of safety is sought and achieved but safety is not intended to be the basic objectives of the activity. It is not a safety activity but rather a transportation activity of which level of safety is a necessary attribute.

- Safety Activities. Activities where safety is a primary objective rather than a performance measure.

- Support activities such as data, planning, R&D, accident investigation and safety analysis which support the achievement of the first two types of safety.

The most common form of departmental program*** or program activity is the first, where funding is decided on criteria other than safety, and where safety is often traded off against other objectives. Transport Canada does conduct certain activities whose primary purpose is transportation safety, but these are much less common.

For the above reasons, the methodology developed here is designed to assist in the establishment of R&D needs related to clearly identified safety programs and objectives only. Multimission type R&D activity of which safety is only one among several other considerations, whether as a spin-off or as a constraint, is not included within the scope of the methodology.

---

* A U.S. DOT study brought out this same problem by asking how much of the construction cost of various widths of highway traffic lanes should be allocated to safety e.g. on 10ft vs. 12ft vs. 15ft wide lanes. Cf. U.S. Dept. of Transportation DOT Allocations for Safety: February 1973 estimated budget authority. Washington DC 1972.

** Transport Canada. "Transportation Safety Analysis of Strategic Change: an appraisal study". Systems Planning Directorate, Strategic Planning Group, November 1980.

*** Program in the Main Estimates (Blue Book) is defined as "a collection of activities having the same objective or set of objectives".

In addition the reference to "all transportation systems" needs some clarification. In broad terms, the modes are air, road, rail, water and multi-model considerations. Within each, however, there may be a number of transportation modes. For example, in road, we might include:

- automobile travel;
- motorcycle travel;
- bicycle travel;
- motor transport;
- inter-city bus;
- urban transportation (bus, streetcar, subway, light rail);
- pedestrian.

We have attempted to provide information applicable to all systems/ subsystems. Necessarily, however, our fact-gathering, interviews and literature review have not encompassed all modes/sub modes in equal depth.

Finally, it should be recognized that the safety mission of Transport Canada necessarily involves policies and programs (including R&D support activities) related to three aspects of the overall safety problem as follows:

- accident prevention;
- accident protection;
- accident recovery (including emergency response).

While the emphasis should be on accident prevention as far possible, experience teaches that accidents do happen, and that the best that can be hoped for is to achieve an adequate level of safety (cf. definition of safety). In this respect, the methodology must be capable of addressing the problem of differentiating needs in all three categories of safety enhancement.

2. INSTITUTIONAL DIMENSIONS OF R&D PLANNING

Design of a methodology to assist in establishing research and development needs in transportation safety must take account of certain institutional realities. In the first place, government initiatives in the field of transportation safety will generally be shaped by the "critical event syndrome", i.e., public (and hence also political) response to catastrophic events. The inevitable conflict of perceived versus "statistical" safety will be dealt with in the following chapter.

Account must also be taken of the institutional environment in terms of the objectives (or mission) of the organization involved, its institutional structure, and the management practices which the method is called upon to assist. For example, transportation research and development at the Federal level is carried out in about fifteen different government Departments and Agencies, the most important of which (in descending order) are the Department of Industry, Trade and Commerce (IT&C), Transport Canada (TC) and the National Research Council (NRC)*. The institutional structure, practices and purposes served are very different in each case. The transportation R&D sponsored by IT&C is largely industrial-type R&D, that commissioned through TC is primarily mission-oriented R&D. Research priorities at the NRC are often determined by other institutions. Transportation R&D is also carried out by other levels of government, by industry and in the Universities.

Finally, the success of any method is always a function of the availability and accessibility of the information required to drive the method and provide the necessary degree of credibility. A brief summary is therefore given at the end of the present chapter on the status of the principal transportation safety data systems currently employed by various Agencies and institutions.

2.1 The Concept of Mission-Dependency

Our interviews in the United States clearly demonstrated the importance of institutional factors for the introduction of formal methods of planning for R&D, particularly in the area of safety. It was found for example that the introduction and successful adoption of scientific or logical techniques of R&D planning is facilitated in certain environments. The key is the organizations "mission-dependency" on R&D, i.e. the perceived significance of the role played by R&D in the performance of overall Departmental mission activity. The stronger the mission-dependency the greater is the likelihood that the organization or Agency is explicitly developed to focus management attention on R&D programs.

A study** of the R&D function in U.S. Federal Agencies, specifically in the U.S. Department of Transportation, found for example that Agencies such as the Department of Defense (DOD), NASA and the Department of Energy (DOE) with high mission dependency on R&D also supported a highly developed organizational structure and a sophisticated tool-kit of management practices and procedures related to the establishment of R&D needs and R&D project identification, evaluation and control. By contrast the U.S. Department of Transportation with a relatively modest degree of mission dependency on R&D (the DOT ranked fifth of the six agencies in the sample) also rated low with respect to the criteria used to evaluate the level of organizational development of the R&D function. The main evaluation criteria were:

---

* Secretariat to the Interdepartmental Panel on Transportation Research and Development. Government of Canada Transportation Research and Development: Situation Report. Ottawa, June 1, 1978. Revised September 6, 1978. Report No. TR&D 78-8.

** U.S. Department of Transportation. Research and Development Activities in the Department of Transportation and Selected Federal Agencies. Washington D.C. Government Printing Office, 1980.

- Science and Technology Advisor Structure;
- Institutional Program Review Structure;
- External Advisory Structure;
- Basic Research Program Structure.

DOT has no Science Advisor to provide guidance on overall R&D program needs, no formal external R&D Advisory Committee at the Department level and no emphasis on Basic Research. While the Department did have a Program Review Structure, it was not dedicated to R&D. By contrast, the DOD's Under Secretary for Research and Development and the DOE's Director of Energy Research both have a statutory basis and maintain basic research offices. In the case of the DOE, there was explicit statutory responsibility to conduct R&D, a Science Advisor with review and program function, a multiple R&D Review Structure, standing External Advisory Committees and a dedicated Basic Research Establishment.

The effect of this on management practices was also revealing. For example, the DOT does not have a long term Departmental R&D strategy plan, an R&D operating plan or even an R&D policy statement to provide guidance to the operating Administrations relative to project selection. R&D planning is essentially "bottom up", each of the operating Administrations selecting and developing R&D projects in accordance with internally-generated policies, plans and R&D strategies. Each has its own (often ad hoc) methods of project identificaion and selection. On the other hand, the Departments of Defense and Energy have both developed and implemented highly sophisticated processes and methodologies designed to manage, plan and control the R&D program effort.

Our own investigations showed that in the specific area of transportation safety R&D planning, attempts have been made by at least five of the eight DOT operating administrations to introduce scientific or at least structured techniques for the identification of R&D needs in the area of safety. The most noteworthy examples are as follows:

- The National Highway Traffic Safety Administration (NHTSA), in conjunction with the Federal Highway Administration (FHWA) published the National Highway Safety Needs Report in 1976. This was the first attempt to develop a coordinated plan for highway safety needs and priorities. This document examines the cost and effectiveness of a wide range of highway safety counter measures.

- The Federal Highway Administration (FHWA) commissioned Stanford Research Institute to develop guidelines for establishing R&D priorities for the FHWA in 1976.

- The National Highway Traffic Safety Administration (NHTSA) has recently completed a review of NHTSA safety priorities, based on cost-effectiveness techniques.

- The Office of Safety and Product Qualification of The Urban Mass Transportation Administration (UMTA) commissioned the Institute of Safety and System Management of the University of Southern California to develop a safety program plan in 1977.

- The Office of Research and Development of the Federal Railroad Administration (FRA) commissioned two studies in 1980 for the purpose of identifying track rehabilitation and maintenance research requirements, primarily in the interest of safety.

- The Office of Research and Development of the U.S. Coast Guard asked the Batelle Columbus Laboratories to develop a Research, Development, Testing and Evaluation Plan for Marine Safety in 1977.

Different methodologies were used, including the adoption of system safety techniques to identify hazard areas. The UMTA safety program plan was implemented to a large extent. However, the remaining plans were superceded and the techniques proposed to develop them have not been adopted in these Agencies. (However, the recent NHTSA priority plan has not been formally rejected by the Administration.) Details of selected methodologies are given in Section 4 of the present report.

2.2 Implications for Safety R&D Planning in Canada

The U.S. experience prompted us to devote some attention to the current situation with respect to organizational development and management for R&D in Canadian Government Agencies, particularly at Transport Canada. Since the Ministry of State for Science and Technology (MOSST) discussion paper of January 1981*, a number of initiatives have been taken to improve the organization and management of R&D in Federal Agencies. In particular, the Office of the Comptroller General (OCG)** and the Auditor General (AG)*** have produced guidelines and within Transport Canada itself ADMSP/DGRD prepared a 5-year strategic plan for R&D**** which proposed five major priority areas for transportation R&D, rail freight, arctic marine, pipelines and urban transportation. Significantly, safety was one of three additional priorities which were assigned across modal lines (the others were communications and control and intermodal systems).

---

* Ministry of State for Science and Technology. R&D Policies, Planning and Programming. Ottawa, January 1981.

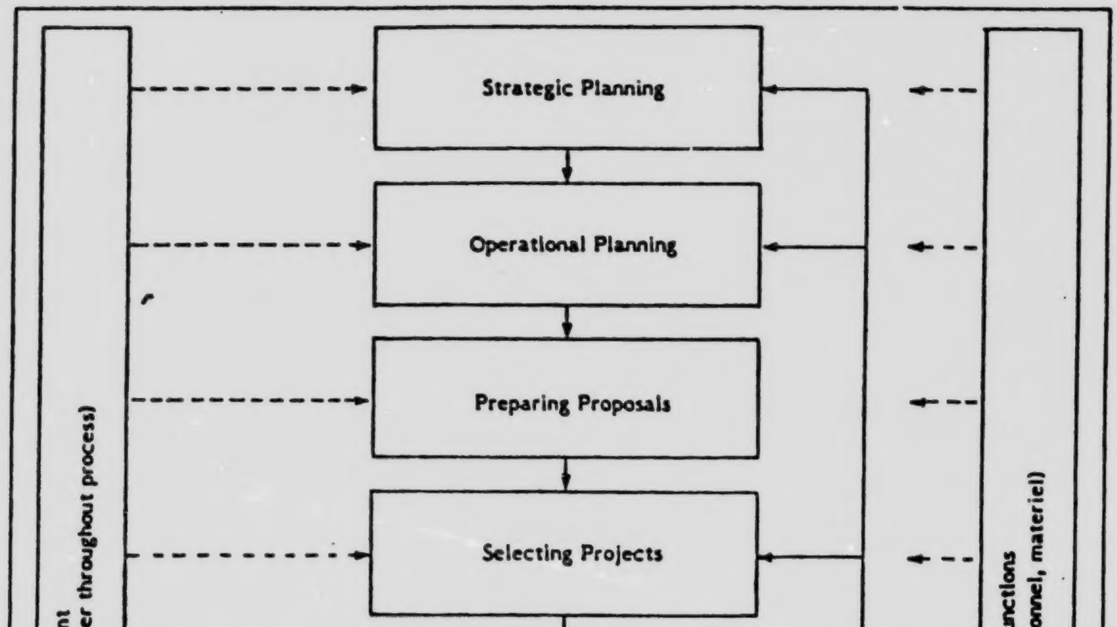
** Office of the Comptroller General. Operational Control of Research and Development in Departments and Agencies of the Federal Government of Canada. Ottawa, October 28, 1981.

*** Auditor General of Canada. "Audit Criteria for the Management of Research and Development in Government Laboratories". In Report of the Auditor General of Canada to the House of Commons: Fiscal Year Ended 31 March 1981. Ottawa, December 1, 1981, pp. 57-63.

**** Transport Canada. A Profile for Federal Government Transportation R&D. Ottawa, February, 1980.

EXHIBIT 2.1

MANAGEMENT PROCESS FOR R&D IN GOVERNMENT LABORATORIES


Client (interacts with researcher throughout process)
Strategic Planning
Operational Planning
Preparing Proposals
Selecting Projects
Operational Control of Projects
Detailed Planning
Final Approval
Implementation
Control
Management Information and Control
Transferring R&D Results
Evaluation
Support Functions (e.g. financial, personnel, materiel)

Source: Auditor General of Canada.
Annual Report: 1981.

No formal review of the Transport Canada organizational and management structure was undertaken for the present study. However, from a recent study of R&D policy developments*, the Department would appear to parallel the U.S. DOT in having a relatively modest mission dependency on R&D and a relatively undeveloped organizational structure for the management of the R&D function.

Like its U.S. counterpart, Transport Canada has no accepted statement of policy or principles which clearly define the Department's interest, role and responsibility with respect to R&D and no internal Science and Technology Advisor Structure or Basic Research Program Structure. The ADMSP/DGRD and Departmental R&D Committees do provide for internal Program Review and an External Structure is provided by the four Modal Advisory Boards.

The present study has, however, taken cognizance of the various proposals that have been made with respect to the four areas of management practice involved in R&D planning, viz strategic planning, long term operational planning, project selection and program evaluation. In this respect the methodology must be designed to fit the management process developed by the AG as illustrated in Exhibit 2.1 opposite.

In particular, the methodology must be designed to accommodate the various proposals that have been made with respect to the R&D project selection process. For example, the AG advises** that selecting projects:

"... is the process through which strategic and operational plans are translated into decisions on specific research projects. Selection of a proposal for a project or a program represents its approval in principle. Frequently outside experts and the client for the research service are involved in the review process.

Proposals should be formally reviewed and approved or rejected using criteria developed by management.

The criteria and decisions should be appropriately documented.

Responsibility for the selection process should be clearly assigned".

For its part, the OCG has this to say about the project selection process***.

"The point of greatest influence in the operational planning of a research activity occurs at the time of project selection. Since the projects selected define the direction which the research effort will take and also the extent and balance it will have, the choice of projects and setting of priorities is critical.

It is for these reasons that the selection of projects and their relative priorities must be carried out in a comprehensive and formal manner. The following are examples of broad categories of selection criteria:

---

* Transport Canada. Towards a Research and Development Policy for Transport Canada. Two volume study prepared for the Research and Development Directorate, Ottawa, June 3, 1982.

** Auditor General of Canada. Op cit. p. 59

*** Office of the Comptroller General. Op cit. p. 6

i) Contribution Towards Achievement of Objectives - government, department, program;
ii) Long term priorities;
iii) Client Needs - industry, department;
iv) Potential Impacts;
v) Technical Factors - skills, facilities;
vi) Funding - total amount, cash flow, timing;
vii) Probability of Success".

Finally, the DGRD study* of 1982 suggests that choice should be governed by certain criteria and guidelines as follows:

RESEARCH PROJECTS	DEVELOPMENT PROJECTS
Selection Criteria	Selection Criteria
- need	- statement of requirement by operational user
- uniqueness	- no available existing source
- cost	- availability of resources for ensuing exploitation
Selection Guidelines	Selection Guidelines

No selection guidelines are given. However, the study** recommends:

- "that project selection guidelines and criteria be developed and incorporated in the departmental policy on TR&D (figure 2);

- within the framework of departmental project selection guidelines and criteria, that the administrations develop in further detail as required project selection guidelines. Selection criteria should reflect those of the OCG;

- that the guidelines or project selection under development by the Sub-Committee on R&D of the Science ADM's Committee be monitored and recommendations integrated into departmental and administration project selection guidelines".

2.3 Transportation Safety Data Sources in Canada

2.3.1 Difficulties with Present Accident Data Bases

Any methodology to assist in establishing R&D needs in transportation safety must be linked to, and use as inputs, any data bases which bear on safety features of the transportation system(s) under study. It appears generally to be the case that, on the whole, available data bases on historical safety performance of various transportation systems are not completely adequate to assist in development of R&D needs, or to provide a measure of the safety improvements achievable through R&D or other system changes. The data relate more to safety management needs than to safety R&D planning needs.

---

* Transport Canada. Op cit. p. 19
** Transport Canada. Ibid. p. 23

The reasons for this include the following:

- Mission Dependency and Jurisdiction. The type and quality of data maintained by a given department or agency will generally be a function of its overall mandate and mission.

For example, CATA has national responsibility to ensure that an adequate level of safety is provided for the national air transportation system. The Aviation Safety Bureau has been empowered to investigate every air accident (Canadian Aviation Safety Board will henceforth assume this responsibility). This has resulted in an extensive and uniform accident data base with up to 900 items per accident on computer file, and a written narrative. On the other hand, demonstrably useful data on "near misses" is not adequately collected.

In the case of road, CSTA has formal national authority only for new vehicle and tire standards regulations. The road accident data base maintained by Transport Canada is based primarily on police reports submitted by the provinces. The records are not uniform and some loss of detail is involved in generating national statistics on a consistent basis.

- The Need for Detailed Accident Reports. There are two main levels of detail for data collection, corresponding to potential uses of the data:

- monitoring data - a "census" of all accidents over many years. These data can help identify any trends and overall problems, and may assist in the assessment of the effectiveness of an agency's policies and programs.

- in-depth, almost "case" studies of groups or types of individual accidents to assess the "causal" chain, or sequence of events leading up to an accident.

It is clear that the second type of accident data would permit the most detailed analysis to identify the specific attributes of the man/machine/environment which are most amenable to change or improvement.

This type of data is, however, fairly difficult to generate, for the following reasons:

- lack of agreed-to procedures to report causal sequences;

- the need to integrate different sources of information (e.g., in road, police and coroner's reports, pavement condition reports);

- possible jurisdictional problems.

- The Costs of Accident Data Collection. The type of data required for detailed analysis can be very expensive to generate. (In the road mode, for example, there are about 5,000 fatalities annually in Canada.)

- The Relative Importance of Various Types of Accidents is Not Always Known. Ideally, this would mean relating the number of accidents of a given type to the relevant amount of exposure (time in vehicle, distance in vehicle, etc.) so that the true probability, or risk of this type of accident can be estimated. Generally, measures of exposure are not known, except in limited instances:

  - aggregate or total exposure is sometimes estimated (e.g., annual fuel consumption is used to estimate total annual vehicle-kilometres);

  - one-time special surveys of the public are carried out to provide estimates of exposure for parties at risk;

  - in some modes, particular segments of trips are well monitored (e.g., St. Lawrence Seaway).

We will discuss exposure measures again in Chapter 3 of this report.

There is a further dimension along which the importance of various types of accidents is not always known - the losses in economic terms. This refers to the actual losses - vehicles, equipment, facilities, investigation resources and lost human work efforts. This group of societal losses is sometimes approximated with a "cost of accidents model" (e.g., air and road).

- Difficulty in Forecasting the Expected Decrease in Accident Losses Resulting from Safety Improvements. Since the causal chain of occurrences is not always understood, and infrequently adequately represented in a given data base, it is very difficult to use the historical (monitoring) data to predict future (improved) outcomes, say, as a result of R&D.

From the above discussion, it is clear that accident data vary in quality and are not always adequate for the purposes of identification of transportation safety R&D needs.

It is beyond the scope of this paper to recommend data collection formats and procedures for each transportation mode. Various studies have previously dealt with data deficiencies [for example, the Ad Hoc Committee on Accident Data Collection (1978) and D.R. Mayhew (1981)].

Certain trends are also evident in various North American jurisdictions:

- statistical sampling of accidents in the road mode in the U.S., followed by intensive investigation of those sampled (National Accident Sampling System (NASS), to be functioning at 75 sites by 1984).

- increased consistency, accuracy and completeness of accident data. [Fatal Accident Reporting System (FARS) in the U.S. since 1975.]

- Safety data base linkage projects to link multiple information files by computer [Utah Department of Transportation has set up system requirements for such a highway project in 1983; work in the air mode is proceeding under the FAA in the U.S. - Aviation Safety Analysis System (ASAS) will be ready by 1985 and will consolidate many sources of aviation safety information to enhance speed, accuracy and capability; CATA in Canada is also reviewing the relationship of its approximately 50 data bases].

In this report, the proposed methodology for identifying transportation safety R&D needs described and exemplified in Chapter 5 includes a step which deals with data needs. This step is built into the early stages of the methodology.

In the following sections, we identify the primary modal accident data bases maintained in Transport Canada (RTC in the case of rail).

2.3.2 The Main Accident Data Bases in Canada

The following is a brief description of the primary modal accident reporting systems in Canada.

- Air Accidents. "Accident/Incident Data System (AIDS)". This data base results from the investigation by federal personnel of all accidents and some incidents. About 900 data items are on computer file. The main types of data include:

- aircraft description;
- pilot/crew qualifications;
- fatalities/injuries (by severity);
- degree of aircraft damage;
- environmental conditions;
- phase of flight;
- search and rescue involvement;
- narrative concerning sequence of occurrences.

These data are computerized. Recently, a costing model has been added to enable the calculation of the economic costs of air accidents in terms of:

- loss of production work efforts (injuries/fatalities);
- aircraft hull damage;
- costs of search and rescue;
- other investigative costs.

It should be noted that for safety management purposes, there are about 50 different data bases maintained by CATA. The work program for the National Air Transportation Safety Program has involved cataloguing these data sources and investigating ways to integrate them.

- Road Accidents. "Traffic Accident Information and Data Base (TRAID)". This data base incorporates reportable accidents, by province and territories, on public roadways. Data are supplied by the provinces based on police reports. Transport Canada converts these data to a homogeneous form and stores it on computer. TRAID is at the level of a "census" of road accidents, with certain basic "monitoring" data such as:

- location, date, time, environment, type of accident;
- vehicle type;
- abstract of driver-related data;
- persons injured.

Causal factors are not consistently recorded - it is often the police officer's opinion.

Another data base in use in Canada is maintained by the Traffic Injury Research Foundation (TIRF). An accident record may include data from coroners' reports, taxicologists' reports, police reports. The cause of accident is based on the police report, while the cause of death is the medical cause, not the external agent (e.g., "ruptured aorta", not "steering column").

- Marine Accident. "Marine Casualty Data Base". This data base is maintained by Casualty Investigations, CMTA. The Canadian Shipping Act specifies which type of casualties are reportable. CMTA investigates and records casualties primarily in the commercial sector. (Pleasure boating is not covered by CMTA). Investigations take the form of Public Enquiries (about 2 per year), Preliminary Enquiry (about 80 per year) and Fact-finding (about 150 per year). All other captain's casualty reports (900-1,000 per year) result in brief summary reports. All casualties are entered on a computerized data base.

The two main classifications of accidents are:

- injury/death as a result of a shipping casualty (collision);

- injury/death on board ship, not the result of a collision (i.e., industrial type accidents).

The data recorded include:

- details of ship, captain, pilot, personnel on watch;
- location, weather, equipment on board;
- descriptive data of the event;
- assessment of cause;
- fatalities and injuries by severity.

The assessment of cause is most detailed in the case of enquiry. Otherwise (in the majority of cases), the cause may be the captain's statement or CMTA's assessment.

- Rail Accidents. All railways in Canada are required to report immediately to the Railway Transport Committee of the CTC, accidents over $750,000 in property damage, personal injury or presence of a dangerous commodity. The cause of the accident is reported. RTC investigates if it feels it is warranted. As in marine, a distinction is made between industrial type accidents and accidents involving moving trains.

Data maintained on the RTC data base include:

- location, etc.;

- the immediate external damaging agent and how the injured person came in contact with the agent (passengers, crew, trespassers, other);

- causes centre around the train-movement, design, equipment failure, slippery surfaces, human error.

2.3.3 Transportation Fatalities in Canada in 1981

As one indication of safety, we tabulate below the fatalities, by mode, as reported to, or investigated by the various modal authorities. We use 1981 as the most recent year. It should be remembered that these are absolute losses only and are not related to measures of exposure.

Air Fatalities (1981)*

Scheduled operations	-
Other commercial	87
Private	85
Total	172

Road Fatalities (1981)**

All fatalities total	5,370
The distribution of this total by victim class:	
Driver	43%
Passenger	29
Pedestrian	16
Motorcyclist	6
Bicyclist	3
Other	3
Total	100%

---

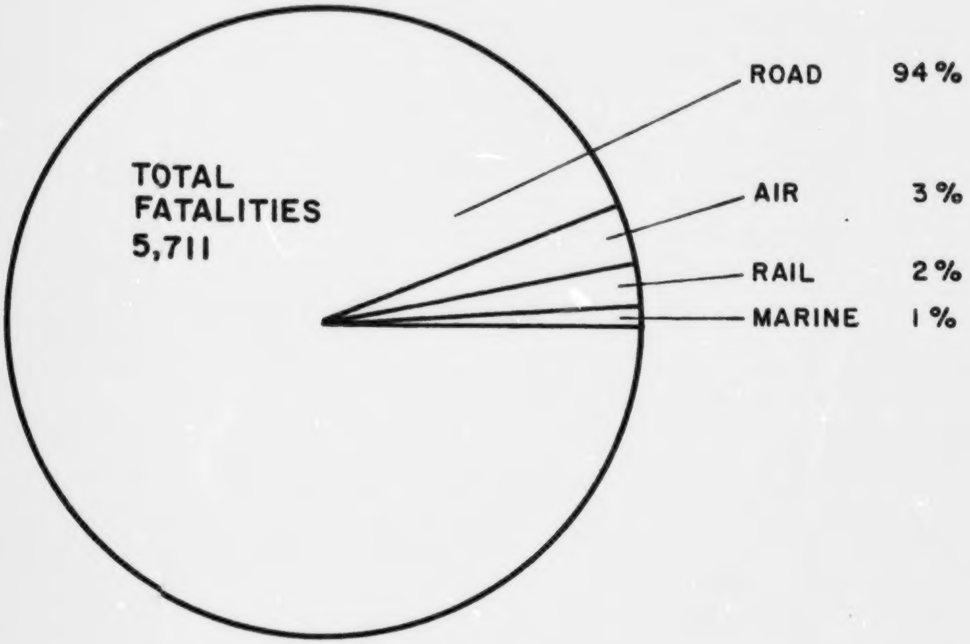
* Aviation Safety Bureau, Statistics, 1970-1981.

** CSTA Statistics, 1960-1981 and CSTA Statistics 1978 for the distribution, which is quite stable over time.

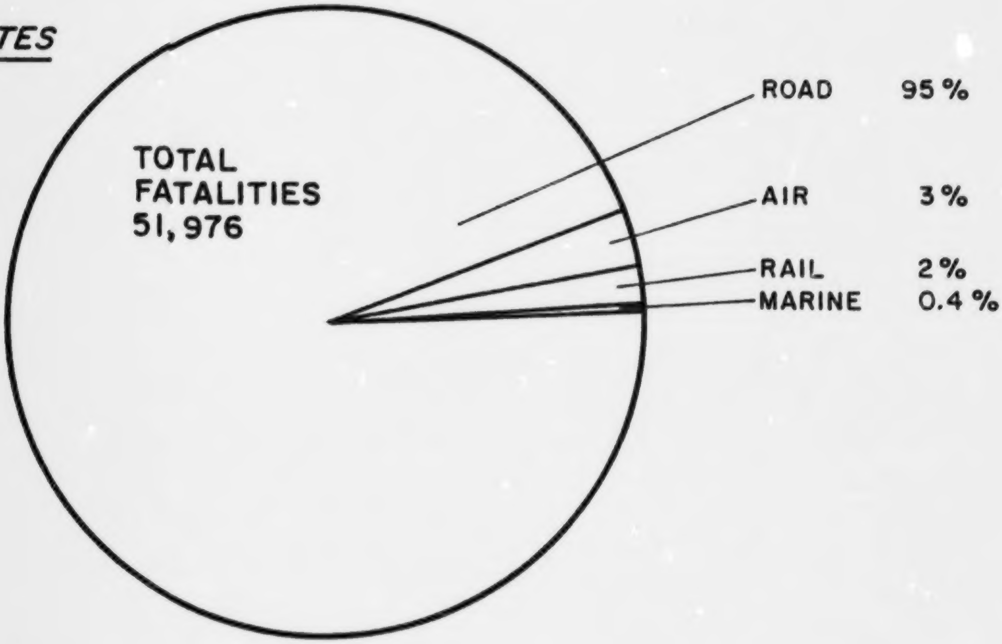
EXHIBIT 3-1

MODAL DISTRIBUTION OF FATALITIES (COMPARISON OF CANADA vs USA, 1981)

CANADA



UNITED STATES



NOTES

ROAD includes all fatalities (vehicular, pedestrian)

TRAIN includes only moving train fatalities

MARINE includes only commercial, collision-related fatalities

Source: Various (as per text).

Marine Fatalities (1981)*

Casualty (collision) related	37

Rail Fatalities (1981)**

Train accidents:	
Employees	18
Passengers	-
Trespassers	36
Others (e.g., at crossings)	78
Total	132

The overall distribution of fatalities is as follows:

	Total #	%
Air	172	3
Road	5,370	94
Marine	37	1
Rail	132	2
Total	5,711	100

This distribution is summarized in the form of a "pie" diagram in Exhibit 3.1 opposite.

2.3.4 Transportation Fatalities in the U.S. in 1981

For the sake of comparison, we show a similar modal distribution of fatalities for the United States for 1981***:

	Total #	%
Air	1,399	3
Road	49,125	95
Marine	196	-
Rail	1,256	2
Total	51,976	100

It can be seen that this distribution is almost identical to the Canadian Distribution for 1981.

---

* CMTA Statistics, 1981 - excludes pleasure boating fatalities.

** Statistics Canada, #52-207, 1981, Table 23)

*** Transportation Safety Information Report, U.S. DOT 1981, Report # DOT-TSC-RSPA-82-4.

3. CONCEPTUAL PROBLEMS OF SAFETY R&D PLANNING

In addition to institutional matters, design of a methodology to assist in establishing R&D needs and to provide a measure of potential safety improvements also raises a number of conceptual issues. These include the measurement of safety, the governing influence of perceived over "statistical" safety, the design level of safety, program versus project planning, accident prevention versus protection and finally, project evaluation. These topics will each be discussed in turn in this chapter.

3.1 The Measurement of Safety

The actual measurement of safety performance of transportation systems is generally expressed in terms of numerical (e.g. accident) frequencies. However, inter-modal comparisons based on numbers is misleading unless these numbers are related to the relevant measure of exposure to risk. In effect, a satisfactory measure of safety requires at least two pieces of information, a numerator describing actual numbers of e.g. accidents, incidents, fatalities, injuries etc., and a denominator linking this information to the most appropriate measure of exposure for the purpose at hand.

There are essentially four basic types of safety exposure measures (denominators) used in the transportation field:

- time-based measures;
- event-based measures;
- activity-based measures;
- population-based measures.

3.1.1 Time-based Measures

Time-based measures of exposure such as passenger or vehicle hours, system years etc. are useful measures of vehicle reliability, but are not very satisfactory indices of safety, since not all time spent in transportation-related activities is of equal risk. For example, this type of measure would tend to neglect accidents which occur during relatively short time periods such as landing or take-off, and would not take account of changes in average speed. A faster vehicle may have a higher accident rate with no increase in accidents, simply as a result of fewer hours of exposure.

3.1.2 Event-based Measures

Event-based measures of exposure such as number of operations, take-offs and landings, entries or exits from harbours etc. make it possible to focus on high risk events. However, in doing so, the measure tends to over-compensate and also makes inter-modal comparisons difficult, if not impossible.

3.1.3 Activity-based Measures

Transportation activity-based measures of exposure such as vehicle kilometers or passenger kilometers is useful in making inter-modal comparison of safety. However, these measures also have a number of disadvantages. They also tend to distort reality where the probability of an accident is not uniform at each stage of the trip. Furthermore, such measures cannot account for differences in capacity and loading factors among the various modes. Finally, information on distance travelled is generally more difficult to come by than time or discrete-event data.

3.1.4 Population-based Measures

Population-based measures of exposure such as numbers of registered vehicles, or vehicles in operation, licensed drivers, passengers or residential population, are not very satisfactory indicators of transportation safety since they do not account for the wide variations in vehicle use. For example, driving a taxi may well be less dangerous than driving a private car even though it shows more accidents per number of licensed drivers or registered vehicles. However, such measures may be useful in comparing the relative contributions of various causes of e.g. death, in health summaries.

3.1.5 Accident Severity

The problem of measurement and evaluation of relative safety is further complicated by the question of accident severity. There is first of all the matter of definition and scope of accident severity in terms of fatalities, types of injury, extent of property damage etc. In practice, there is no commonly accepted accident severity scale. In addition, some framework must be established to account for differences in the frequencies of the various accident severity types across the different modes.

3.1.6 Choice of Safety Exposure Index

A Batelle study* has pointed out that in practice, the choice of a particular index of exposure or accident severity is often motivated by the desire to present a particular system or facility in the best possible light. In addition, choice may be determined by the availability of data. Review of existing data sources shows that time series transportation safety data typically include little more than the number of fatalities together with some descriptive statistics such as passenger-kilometers of travel and perhaps trip characteristics such as average trip length. One-time special surveys are often required to provide more in-depth understanding.

Most importantly from our point of view, choice would depend on the purpose to be served. Safety may be viewed from the perspective of the passenger or the shipper (cargo), of the vehicle manufacturer, of the operator or of society as a whole (represented by the government). The passenger is primarily concerned by the prospects of his own death or serious injury, the shipper is interested in the risk of loss, the manufacturer in the prospect of mechanical failure, the operator to loss and damage to the vehicle. Society or the government would be interested in all these various elements of risk, but it is not always clear where the emphasis is to be placed or more importantly, how the emphasis should be determined.

---

* E.S. Cheaney et al. Safety in Urban Mass Transportation. Columbus: Batelle Columbus Laboratories 1975. Prepared for the U.S. Department of Transportation, Urban Mass Transportation Administration, UMTA-RI-06-005-75-1.

We show a few examples of exposure indices currently used. These indicate that inter-modal comparisons are very difficult, even if trying to compare, for example, safety of passenger travel.

- Air Mode. The exposure index provided by the Aviation Safety Bureau is "100,000 hours flown". It was noted above that this measure gives too little weight to the dangerous part of the trip, takeoff and landing. Additionally, this is a measure of aircraft exposure, and not personal exposure. That is, these hours would have to be factored up by the number of crew/passengers on board. The statistics tabulated by ASB show the simpler measure, "fatal accidents per 100,000 hours". The following shows these values for 1980:

	Fatal Accidents per 100,000 Hours Flown (1980)*
Scheduled operations	0
Other commercial	1.63
Private	2.77
All operations (weighted average)	1.76

These data appear to indicate that private flying is the most dangerous in terms of fatalities. There has been a slight decline in the overall indicator over the last decade, based on the time series for 1970-1980.

- Road Mode. The exposure indices used by CSTA** are "100 million vehicle-kilometres" and "100,000 population".

	Fatalities Per 100 million Vehicle-Km	Fatalities Per 100,000 Population
1970	4.0	23.9
1975	3.4	26.7
1980	2.7	22.8

On the assumption that the vehicle-km measure is accurate (usually based on average fuel consumption), the road mode has become safer over the last decade. On a population basis, there is also a slight downward trend. However, the vehicle-km activity measure, as noted above, does not take account of vehicle loading differences. The population measure does not take account of changes in vehicle usage. Thus, the degree of safety improvements, apparently shown in the data above, is not entirely certain.

- Marine Mode. For commercial marine transport, no overall exposure index can be supplied by CMTA, except in very specific instances, such as passage through the St. Lawrence Seaway or during pilotage movements.

---

* Aviation Safety Bureau Statistics, 1970-1981

** CSTA, Statistics, 1960-1981

- Rail Mode. Differing exposure indices are used in rail:

  - billion gross ton miles (BGTM) or ton kilometres;
  - car miles or car kilometres;
  - train miles or train kilometres.

The railways themselves express their safety performance in a variety of ways, for example:

- train accidents per BGTM;
- % of unsafe cars (determined by quality control check);
- car-miles per hot box.

In terms of train kilometres*:

	1977	1981
Fatalities	138	132
Train kilometres	140 million	134 million
Fatalities per million train kilometers	1.0	1.0

This ratio has not changed over the four-year period shown above. On a 100 million vehicle kilometre basis as in road, the value would be .01 fatalities per 100 million vehicle km., compared to 2.7 in 1981 for road.

It should be remembered that the rail fatalities include crossing accidents. In this case, the number of fatalities per crossing or 1,000 crossings would be more relevant than relating fatalities to train kilometres.

3.1.7 A Universal Failure-index

It seems clear that from the point of view of the present study, it would be useful to have some overall general-purpose index of transportation safety applicable to all modes of transportation. The criteria for development of such an index would seem to be:

- general applicability for the measurement of safety across all modes;

- capable of identifying and measuring discrete hazard areas in the various modes;

- capable of measuring the safety improvements achievable through R&D.

---

* Statistics Canada, #52-207, 1981, Tables 10 and 23

The development of such a safety index is a complicated procedure from a theoretical point of view. One such effort is by Byun*. The failure index developed in this paper is intended to apply to all modes and allow inter-modal and intra-modal comparisons. The procedure involves considering the major "risk environments" in each mode (e.g. takeoff, cruise, landing for the air mode), and, using probabilities of traversing each environment successfully as well as the average severity in an unsuccessful traversal of each environment, then calculating the average (expected) severity over the entire trip.

Using only one severity (fatality), and various other (somewhat arbitrary) simplifying assumptions, the author found the following:

- air is less safe than intercity bus or rail for trips less than 2,400 km (4,800 km if the aircraft makes one stop);
- air is less safe than auto for short trips;
- intercity bus has a slight advantage over rail.

Further work would be required to develop this index for practical use and to be applicable not only to fatalities, but also injuries.

3.2 Perceived and "Statistical" Safety

We have already mentioned how Government program and R&D project initiatives in the field of transportation safety, as in other fields of safety, are susceptible to the "critical event syndrome", the political hazards that result from the occurrence of catastrophic or potentially catastrophic events. A good case in point is the derailment which occured at Mississauga on November 10, 1979 and led to the recommendations of the Grange Commission Enquiry. However, events such as these only serve to highlight the much more general and pervasive tendency in human nature and society to base decisions (and allocate resources) not on the actual or "statistical" probabilities of untoward events but on the perceived risk of occurence. This often results in a curious double standard with respect to safety in our society. For example, while there is increasing concern for the safety of new technologies, particularly in the field of nuclear power generation, there is widespread apathy or even resistance to accepting correspondingly high safety standards for activities on the roads or in the home where the risks of fatalities and injuries are many times greater. Transport of gasoline by truck appears from all the statistical evidence to be an overwhelmingly greater threat to life than transport of radio-active materials, but public opposition to the latter is overwhelmingly greater.

---

* cf. Joonho Byun et al. "Transportation Safety Index Applicable to All Modes". Transportation Research Record No. 709. Transportation System Safety and Project Analysis. Washington, D.C. 1979.

There are a number of reasons for this. People will normally accept higher risk in voluntary than in imposed activities. A mountain climber will accept risk that a miner would not. People also tend to weight less heavily risks that are familiar. It is easier for some to cross a busy street than to get into an airplane. Again, people have a tendency to overestimate the probability of highly memorable or easily imagined events (sensational media coverage is obviously a contributing factor here). There may also be comfort in numbers. A person may prefer to be part of a group of fifty, half of whom are to be fired than of a group of two, one of whom is to be fired.

These individual attitudes to risk inevitably impact the manner of public decision-making about investments in safety. For example automobile safety priorities could be affected by the seemingly greater degree of personal control, because media coverage of air disasters makes the image more vivid and because the risk and thrill of driving have a greater element of voluntarily - assumed danger about them*. In addition, experience in the road mode suggests that attitudes to risk also play a vital part in the success of any proposed countermeasures.

3.3 Levels of "Acceptable" Risk

Attitudes to risk will also determine the levels of risk that society is willing to accept. This may differ between modes and even between elements within a single mode. If absolute safety (no incidents, accidents, fatalities or injuries) is not achievable, what level of safety is "acceptable" before anything is done about it. This is clearly grist for the mill of any "scientific" attempt to establish R&D needs. This problem is complicated by the fact that there are two sets of risk involved, the risk of an accident (i.e., the level of "primary safety") and the risk of death or injury once an accident has occurred (i.e., the level of "secondary safety").

This issue has been the subject of considerable debate**. The notion of "acceptable risk" has not generally been applied in the transportation safety area, although formal target setting is often implied in the road mode. For example in Britain guidelines exist to aid decisions about the adoption of various road safety measures and these might be considered to imply that below certain levels of risk there is no strong case for spending public funds on countermeasures***.

3.4 Program versus Project Planning

In designing a method to assist in establishing R&D needs in transportation safety, a distinction must be drawn between program planning and project selection techniques. In the U.S. Department of Transportation, planning methods in the safety area have largely focussed at the level of safety program planning or safety R&D program planning. At the U.S. Coast Guard for example, a system safety method was used to develop a research, development, testing and evaluation program plan, which included the identification of individual project areas, projects and tasks. In effect, project selection cannot be viewed in isolation of overall program and institution mission needs.

---

* cf. A.R Dobell. "The Arithmetic of Risks: analytical problems and political solutions". Policy Options Politiques, June 1980.

** cf. Richard C. Schwing and Walter A. Albers, Jr. (Eds.) Societal Risk Assessment: How Safe is Safe Enough? New York, Plenum Press, 1980. Also see Vincent T. Covello. "The Perception of Technological Risks: A Literature Review". Technological Forecasting and Social Change, August 1983.

*** cf. Barbara E. Sabey and Harold Taylor. "The Known Risks we Run: The Highway". Ibid, p. 45.

3.5 Accident Prevention versus Accident Protection

The application of a system safety or other logical approach to the management of transportation safety R&D planning must necessarily deal with the trade-offs that are involved in the choice between accident prevention (reducing the risk of accidents) and accident protection (reducing the risk of death, injury or other damage once an accident has occurred). This is the issue of primary vs. secondary safety alluded to above.

This issue is complicated by two principal factors. In the first place two sets of causal chains are involved or rather the total causality has to be looked at in two parts. Identification of safety problem areas (or hazard areas) must be based on the event chain leading to an accident. However, the identification of project areas (i.e., remedial action) must take account of both the event chain leading to the accident and the event chain determining the severity of the consequences of a given event.

Secondly, when considering the remedial potential of R&D projects (once the safety problem areas have been determined through analysis of hazards etc.), it must be remembered that the most effective remedy may not necessarily be related directly to the main causes of the accident itself. This is perhaps most easily seen in the road mode where, for example, human behaviour may be influenced more readily by highway engineering techniques than by education, training or law enforcement*.

3.6 Project Evaluation

It is not the purpose of the present study to address the problem of R&D project evaluation. However, the approach used to target areas of R&D need through hazard identification and assessment of the safety improvements achievable through R&D, may have some eventual application in this area. This could (eventually) be achieved in part through the development of safety performance measurement techniques, in part by the potential offered to develop more quantitative assessments of risk.

---

* cf. Organization for Economic Co-operation and Development. Hazardous Road Locations: Identification and Counter Measures. Paris, OECD, 1976. Also: G.R Watts and A.R. Quinby. "Aspects of Road Layout that affect Drivers' Perception and Risk Taking". Transport and Road Research Laboratory, Laboratory Report No. 920, Crowthorne, 1980.

4. SYSTEMATIC TRANSPORTATION SAFETY PLANNING METHODS

4.1 Introduction

In the competitive market-place, R&D activities are sponsored by an industrial organization either to create new markets, to enlarge existing markets or to improve the profitability of its operations. R&D needs are determined by the perceived needs of the market-place and the activities of the competition, usually determined through careful market research. However, in the public sector as we have seem in Chapter 2, R&D needs are largely tied to departmental mission and program objectives, and may be created by the need to support:

- Departmental regulatory activity;

- Departmental operating functions; or

- New technologies that would not otherwise find a sponsor in the private sector.

In all cases, R&D needs are mission related and tied to individual regulatory, operational or industrial-type programs. In the mission field of transportation safety, this situation may be represented graphically, with the help of Exhibit 4.1 overleaf.

Ideally, the Departmental safety mission is derived from the overall Departmental Mission. However at this level, the Safety Mission can only express a rather general perception of a need for enhanced transportation safety. It must be translated into a series of more clearly defined remedial actions (or countermeasures), packaged in the form of individual regulatory, operational and industrial-type safety programs.

In this connection, a wide range of possible actions (or "levers") may be available. In the regulatory area for example, safety may be enhanced through the development of regulations and standards, involving control and implementation through various certification, licencing, inspection and enforcement activities and programs of public education. Government operations such as Search and Rescue, Air Traffic Control and Coast Guard functions are often used to promote safety, and certain Industrial programs may also be sponsored in the interests of transportation safety.

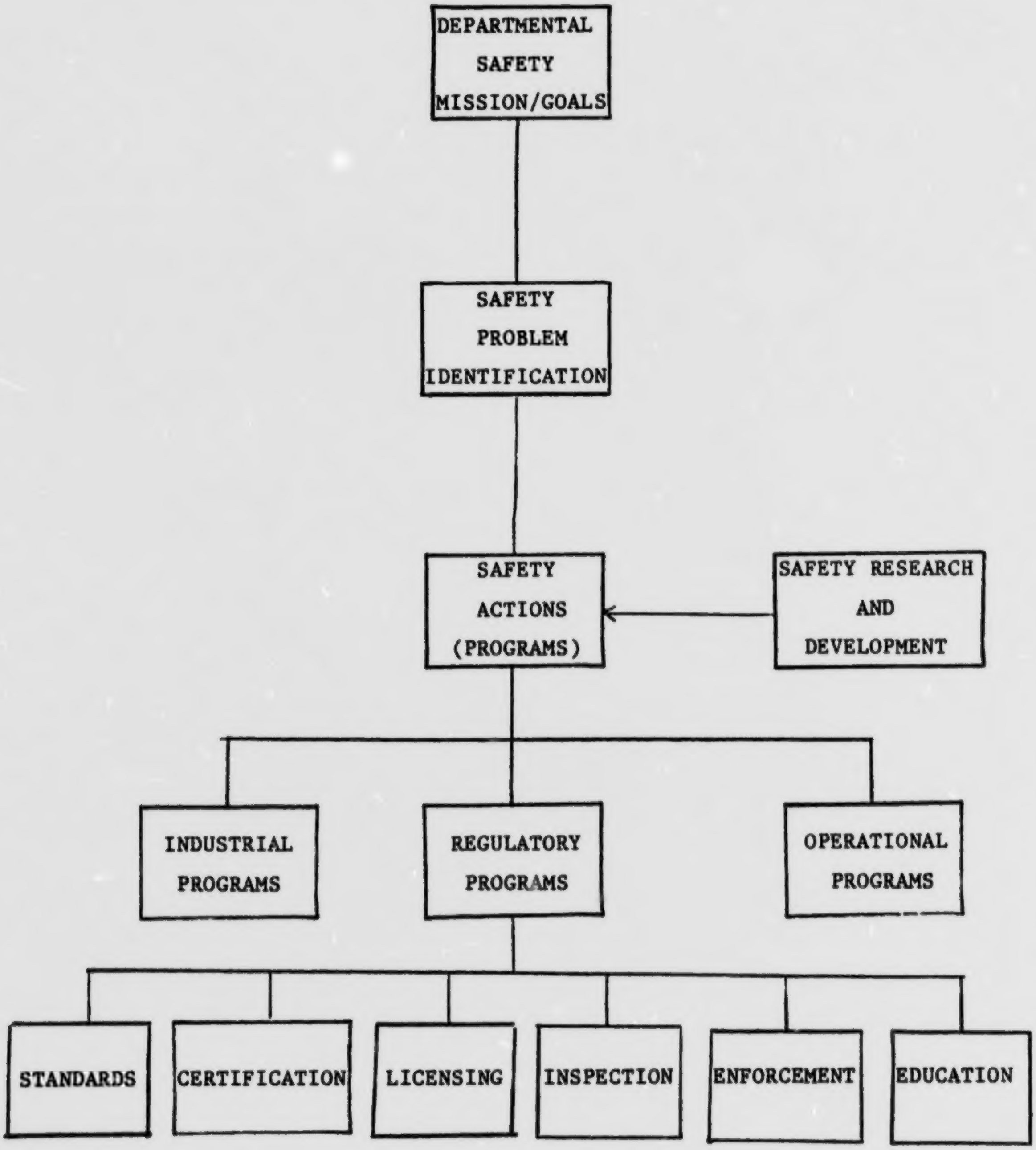
The Research and Development activities of Government are generally treated as one of several possible inputs to these various program functions.

In this manner, the establishment of R&D needs is intimately related to the establishment of Transportation Safety Program needs. As a support activity, however, R&D is methodologically one step removed from the safety problem areas, and the establishment of R&D needs in transportation safety follows from a consideration of all the various safety actions that may be available to the public decision-maker. In effect, the establishment of R&D needs involves a two-stage procedure as follows:

- identification of transportation safety problem areas;

EXHIBIT 4.1

SAFETY R&D SUPPORT OF AGENCY
MISSION OBJECTIVES AND PROGRAMS


DEPARTMENTAL SAFETY MISSION/GOALS
SAFETY PROBLEM IDENTIFICATION
SAFETY ACTIONS (PROGRAMS)
SAFETY RESEARCH AND DEVELOPMENT
INDUSTRIAL PROGRAMS
REGULATORY PROGRAMS
OPERATIONAL PROGRAMS
STANDARDS
CERTIFICATION
LICENSING
INSPECTION
ENFORCEMENT
EDUCATION

- determination of the aspects or segment of the problem that is susceptible to an R&D solution.

In practice, Transportation Safety Programs are inherited from the past and hence "given" in the sense of being ongoing, rather than built up from scratch. Both the programs themselves and the R&D component are determined not from a logic analysis of safety problem areas, but rather as a result of various practical or political considerations linked to parts of a problem or the manner in which the problem is perceived.

Ideally, however, the Transportation Safety Programs themselves, involving the gamut of possible remedial actions, should be built up on the basis of a systematic identification of safety problem areas. This type of approach has in fact, been tried by certain Agencies of the U.S. Department of Transportation and it is the purpose of the present chapter to review state-of-the-art approaches and methods which have been developed to assist in providing a more rational basis for the planning of safety remedial actions, including R&D in safety. It should be noted however, that methodology was not generally the major concern in these studies. In addition, most of the methods were developed in the course of planning exercises designed either to prepare safety program plans or to develop all-purpose R&D plans. Only one of the major studies reviewed below was specifically concerned with the planning of transportation safety R&D. However, the methodology developed and employed in these studies may all be considered relevant to the R&D planning process as described below.

4.2 The R&D Planning Process

A number of key decision elements or phases may be identified within the overall decision process related to management planning, administration and control of research and development. These include decisions related to the identification and/or development of:

- R&D susceptible problem areas;
- R&D project proposals;
- R&D selection and resource allocation procedures;
- R&D monitoring and evaluation techniques and procedures;
- R&D co-ordination mechanisms.

Decisions at each stage may involve various levels of management, depending on the approach taken towards management of the R&D function.

Results of the present study are targeted primarily at the first phase of the planning process, although in evaluating the safety improvements achievable though R&D and other system changes, certain aspects of the next two decision elements must also be considered.

The first three phases in the R&D management process are clearly highly interrelated. The identification of problem areas automatically provokes an imaginative (and usually rather costly) "wish list" of potential transportation safety actions, including R&D projects. However, budget constraints usually make it necessary to be selective about the allocation of resources to the solutions proposed. Following budgetary approval (i.e., during the actual implementation phase of projects), the need arises for techniques and procedures to assist in measuring and monitoring performance and evaluating the safety improvements actually achieved as a result of individual R&D programs or projects. Finally, management must also concern itself with the task of coordinating the efforts of different line organizations, both with respect to overall strategic mission objectives and also with respect to work conducted in parallel by other departments and organizations with similar missions.

The studies reviewed below have been chosen to illustrate methods applied more specifically to the identification of transportation safety problem areas, and to the development and selection of transportation R&D projects. Little attention has been given to the resource allocation process or to mechanisms of R&D control and co-ordination.

4.3 The National Highway Safety Needs Reports of 1976 and 1981

The National Highway Traffic Safety Administration (NHTSA) safety mission is both preventive ("to increase highway safety"*) and protective ("to reduce the deaths and injuries occurring in such accidents"**). It is carried out by means of two major groups of programs, highway safety programs or programs related to the driver and vehicle occupants and non-occupants (e.g. pedestrians) and motor vehicle safety programs or programs related to the vehicle itself. The Agency mission is complicated on the highway safety side by the fact that it is State and local units of government that actually operate highway safety programs. It is complicated on the vehicle safety side by the numbers and types of vehicles involved, design and tooling lead times, and the economic aspects of manufacturing and marketing.

This two-fold mission emphasis and the multiplicity and fragmentation of jurisdictions and system elements, has had a profound effect on the manner of defining and establishing program needs, including R&D program needs in safety. In this situation, programs are clearly needed as much in the area of accident protection as in that of accident prevention, and this has tended to focus management attention on the accident itself and its aftermath, rather than on implementation of a comprehensive "system safety" plan for the "highway transportation system". While preventive accident countermeasures are, of course, much in evidence, these are generally developed as a result of accident analysis, rather than as a result of a probabilistic analysis of the hazards involved in "accomplishing the mission" of highway transportation.

The National Highway Safety Needs Report of 1976*** was the first attempt to develop a rational framework for the identification and development of highway safety needs in the form of countermeasures. It was prepared at the request of Transportation Secretary Coleman, Jr. in response to a directive by the U.S. Congress to provide a basis for evaluating the continuing highway safety programs authorized under Title 23 USC. The final product however, was in fact a new priority list of countermeasures, (specifically excluding any R&D component), based on a careful analysis of highway safety problem areas. While this study did not deal with safety R&D Programs or projects as such, it did develop methods with which to come to grips with three main issues or areas of interest as follows:

---

* 23 USC 4001 - Highway Safety Act of 1966.

** 15 USC 1381 - National Traffic and Motor Vehicle Safety Act of 1966.

***United States. Department of Transportation. National Highway Safety Needs Report. Report of the Secretary of Transportation to the United States Congress pursuant to Section 225 of the Highway Safety Act of 1973. Washington, D.C. Government Printing Office, April 1976.

- identification of highway safety problem areas;

- identification and development of relevant highway safety countermeasures;

- prioritization of countermeasures through analysis of benefits and costs.

The output of the report was in part a response to the secretary's complaint with respect to:

"the paucity of information by which to guage what improved levels of performance may be realized with different expenditure levels ... In the past, we have been unable to project with any degree of precision where the government can realize the most benefits for the next marginal dollar of expenditure or what aggregate national benefits can be realized at any predetermined level of expenditure".*

The study thus attempted to identify those countermeasures that would provide the user States with the greatest return on the dollar invested. In this connection, return or benefit was measured in terms of the number of fatalities and injuries forestalled by a particular countermeasure.

As a result of a request from the House Public Works Committee, the NHTSA produced an update of the 1976 study in 1981**, designed to identify the highway safety needs of the decade of the 1980's. This Report is somewhat more limited in scope to the extent that it did not include FHWA programs. However, the methodologies and measures used in both studies were practically identical.

4.3.1 Identification of Highway Safety Problem Areas

The two Highway Needs Reports both recognized that the concept of "need" implies the existence of a problem which takes the form of loss or deficiency with respect to some ideal state of affairs or standard. A solution can therefore only be sought in the context of established safety goals and an effective action plan for their achievement. Exhibit 4.2 illustrates this relationship between problem identification and the selection, implementation and evaluation of the appropriate accident prevention and protection countermeasures.

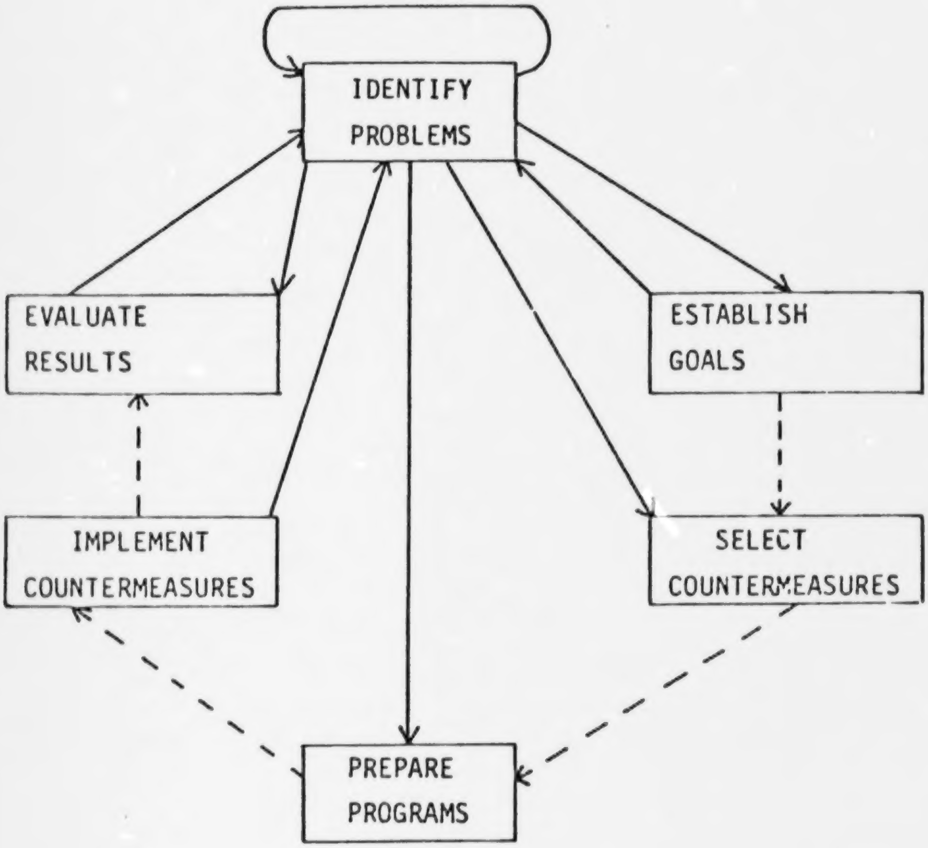
---

* U.S. Department of Transportation. Statement of National Transportation Policy. Washington, D.C. September 1975, p.22.

** United States. Department of Transportation. Highway Safety Needs Study 1981 Update of 1976 Report to Congress. Prepared by the Office of Program and Demonstration Evaluation, National Highway Traffic Safety Administration. Washington, D.C. 1981. NTIS PB 83-158584.

EXHIBIT 4.2

THE ROLE OF PROBLEM IDENTIFICATION IN THE SYSTEM'S APPROACH TO PROGRAM DEVELOPMENT


IDENTIFY PROBLEMS
EVALUATE RESULTS
ESTABLISH GOALS
IMPLEMENT COUNTERMEASURES
SELECT COUNTERMEASURES
PREPARE PROGRAMS

Source: United states Department of Transportation.
Problem Identification Manual for Traffic Safety Programs; Volume 1, Washington, D.C.
National Highway Traffic Safety Administration,
December 1976.

During the mid-1970's, NHTSA devoted considerable attention to safety management and this led to a new Federal program assistance approach, based on problem identification, called the Highway Safety Management System Plan (HSMSP). By 1976, the Office of State Program Assistance had produced a useful Manual designed to provide State Highway traffic safety management personnel with practical methodological/statistical tools to assist in the establishment of highway safety needs*. This procedure is essentially the approach taken to identify the safety problem areas for the Highway Needs Study. In this respect, "a problem may be viewed as any undesirable situation which is directly or indirectly related to accidents, drivers or the driving environment".

Two types of problem are considered:

- impact problems;
- systems support problems.

Impact problems are problems that can be related to accident reduction through the application of countermeasures. Systems support problems on the other hand, are administrative or technical problems related only indirectly to accident reduction e.g. inadequate systems (including record systems), technologies, etc. While the Highway Needs Study was concerned exclusively with impact problem identification (thereby specifically excluding R&D), it did in fact provide a good illustration of the application of the new problem identification techniques.

The principal characteristics of the NHTSA approach is that it is based on the potential utility of existing traffic records information. In effect, it is an inductive data analysis approach to targeting those areas of accident occurrence which are over-represented with respect to either geographic location or to the driver/vehicle population as a whole. Potential trouble spots could include for example alcohol, youth drivers, roadside or roadway hazards, high accident locations, defective vehicles, etc. Various levels of analysis may be identified. Level I for example, is the first or primary cut across the data to isolate general problem areas. Level 2 is a subsequent cut which further refines the possible problem situation, and this process may be continued until problems become specific enough to allow for the formulation of countermeasures.

4.3.2 Identification/Development of Highway Safety Countermeasures

The identification and development of highway safety countermeasures is in large measure a natural fall-out of the problem identification process. "Not only does a list of real and potential problem areas become apparent, but a set of potential remedies evolves as well, providing a basis for organizing and establishing priorities." Problems and solutions (remedial actions) are considered as inputs to the prioritization process, and these emerge from reviews of the literature (including reviews of existing data), as a result of inputs from States and local surveys , and from expert opinion organized in the form of a Delphi "Panel of Experts".

---

* United States. Department of Transportation. Problem Identification Manual for Traffic Safety Programs. Two volumes. Prepared by the Office of State Program Assistance, National Highway Traffic Safety Administration. Report No. DOT HS-802084. December 1976.

The identification and development of relevant highway safety countermeasures was assisted by an examination of the forecast levels of fatalities and injuries over the following 10 year period, based on accident trend data and inputs from the three sources of input already mentioned above.

4.3.3 Selection/Prioritization of Countermeasures

A limited benefit/cost framework was established with which to evaluate the effectiveness of the various countermeasures that were developed to meet the major problems that could be foreseen over the 10 year time horizon. The effectiveness of a countermeasure was judged to reside in two factors:

- its own unique value as a deterrent of either the number of accidents or their severity;

- the size of the population affected by its deployment.

The deterrent values were estimated by reference to experiments and tests appearing in the literature . Although carefully sifted so that only empirical or statistical data possessing some degree of scientific objectivity was used, the deterrent values remained, for the most part, highly judgemental. The size of the population affected was estimated from statistics or sample surveys available though the Department of Transportation or the National Safety Council, and raw or analyzed State traffic statistics. The panel or experts was used to further refine the estimates of safety benefits.

The potential costs of each countermeasure were estimated on a national basis using survey data acquired by interviews with officials in 20 States and 593 local jurisdictions. Costs included initial costs, capital costs, recurring costs and user costs, all of which were estimated in terms of constant 1974 dollars over the 10 year period and converted to their present value at a rate of 10% p.a.

The cost-effectiveness of each countermeasure was largely measured and evaluated in terms of the dollar cost of saving lives. While this does provide a ranking of alternatives, it does not necessarily reflect benefit/cost in each region, since potential savings of lives varies widely, in each case. However, this sort of analysis does provide sufficient insight to target the candidates most likely to produce the greatest payoff in terms of overall safety benefit (fatalities and injuries forestalled) for the direct costs of the countermeasures involved.

In the years that followed, considerable progress was made, particularly at the National Highway Traffic Safety Administration (NHTSA), in developing and refining the methodology developed in the mid 1970's, more specifically as a result of improved accident data and the completion of the National Accident Severity Study (NASS) which made it possible to quantify the dollar impact of different levels of injury according to the Abbreviated Injury

Scale or AIS. This made it possible to estimate benefits in terms of dollar savings in "total human harm" rather than simply in terms of fatalities and injuries avoided.*

It is recognized that these methodologies are only a first step. In fact, one of the recommendations of the 1976 study was that, "a more rigorous means should be developed using this study as a point of departure, for stating goals, identifying needs, and measuring concomitant results within a changing traffic safety setting". However, the emphasis was placed on improving the process of countermeasures development and evaluation rather than on the process of problem identification.

4.4 The National Highway Traffic Safety Administration 1983 Safety Priorities Plan

Since the National Highway Safety Needs Study of 1976, progress in developing and refining in-house methods of safety program planning has been greatly facilitated by the work of the National Centre for Statistics and Analysis, an in-house group charged with the management and development of the three main sources of highway safety information, the Fatal Accident Reporting System (FARS), the National Accident Sampling System (NASS), and the National Crash Severity Study (NCSS). In April 1983, the NHTSA finally produced the long-awaited Safety Priorities Plan which covers all the NHTSA areas of Program responsibility, including R&D support in safety**. The planning process is similar to the traditional NHTSA approach to the selection of Program priorities. The main ingredients include:

- targeting of major safety problem areas through accident analysis;

- development of alternative program solutions;

- selection and prioritization of program alternatives (including R&D) based on a largely judgemental evaluation of benefits and costs.

The planning document specifically warns against seeking to quantify all the consequences of safety actions. In fact, the NHTSA has adopted a policy of not trying to express all benefits and costs in terms of single units such as dollars, on the basis that:

- they are not required to do so by governing statute;

- it would result in unnecessary levels of uninformed controversy (e.g. in value of life estimation);

---

* Cf. A.C. Malliaris et al. "A Search for Priorities in Crash Protection". In Society of Automotive Engineers. Crash Protection SP-J13: Proceedings of the International Congress and Exhibition. Detroit: Author, February 22-26, 1982.

** United States. Department of Transportation. Planning for Safety Priorities: 1983 Safety Priorities Plan. Washington D.C. National Highway Traffic Safety Administration Report No. HS 806 399. April 1983.

- many consequences are impossible to reduce to unit values;

- single unit measures such as dollars overly simplify complex public policy issues;

- an "efficiency test" is not necesarily the best criterion to evaluate the potential for reducing individual harm from highway accidents.

The policy was therefore to quantify wherever this was useful for purposes of informing judgement, but to stop short of attempting to express every aspect of a problem in quantitative terms, particularly when these are reduced to single units of expression such as dollars.

The following is a somewhat more detailed description of the methodologies and procedures used in this Plan to assist in defining highway safety problem areas and in establishing programs and program priorities to deal with them.

4.4.1 Identification of Problem Areas

Three main tools of problem analysis were used to assist the NHTSA management in identifying problem areas:

- statistical analysis of accident and exposure files;
- trend analyses;
- forecasting.

The statistical analysis of accident data and accident exposure data followed the traditional procedures originally detailed in the NHTSA Problem Identification Manual. While this procedure was to some extent designed to identify the various factors involved in the accident event (e.g. alcohol, young drivers etc.), the Plan document uses the term "contributing factor" rather than "cause", and provides a graphic example to illustrate the futility of developing remedial actions based on a strictly causal analysis. A scenario is given which describes the hypothetical case of a drunken driver, not using his safety belt, travelling at night, in the rain, in a car with a broken headlight and faulty brakes, on an unlit, poorly marked roadway without breakaway sign posts. The driver sees something in the roadway, brakes, skids, hits the nonbreakaway sign, and is killed when his chest smashes into the steering column.

The issue is then raised as to the cause or causes of death? Was it the excess of alcohol which slowed the driver's perception and reflexes? Was it the broken headlamp which didn't provide enough light ahead of the vehicle? Was it the faulty brakes which couldn't prevent the vehicle from skidding into the sign? Was it the wet pavement? Was it the rigid signpost? The lack of roadway lights? The not very "forgiving" steering column? The absense of seat belt protection? If any one of these factors had not been present, death may have been avoided.

The Document goes on to suggest that determination of "cause" may not be relevant to the development of countermeasures. Darkness and inclement weather are the only non-controllable aspects of this situation and the safety of the driver could have benefitted from a wide range of accident prevention and accident protection measures, including programs to prevent drunk driving, enforce seat belt usage, make the highway more "forgiving" and so forth. However, the NHTSA did recognize that not all the "contributing factors" are of equal probability or importance, and detailed statistical analysis was performed to identify the major driver, vehicle and environment-related contributing factors, both with respect to the accident itself and the "second collision", in this case the driver hitting the steering column. In all cases, factor analysis of this kind relied on the available sources of date mentioned above.

In addition to this traditional statistical analysis of accidents, the NHTSA made greater use of historical trend analysis to identify emerging problem areas. For example, the fact that motorcycle deaths increased during the period 1974-1980 from 7% to 9.7% of all highway deaths, highlighted an increasing motorcycle fatality problem and prompted further investigation into causes.

Finally, the current plan effort made greater use of technological and other forecasting techniques as tools to predict problems that might not yet exist to a significant degree at the present time. For example, future changes in vehicle mix (e.g. projected increases in the proportion of light trucks on the highway) and vehicle characteristics (e.g. potential increased weight differentials between highway vehicles due to the increasing numbers of smaller passenger cars) were highlighted as new areas of potential concern.

In summary, the NHTSA took an eclectic rather than a "systematic" approach to the identification of highway safety problem areas, using a wide variety of statistical and judgemental techniques. The NASS data file and special studies were used to identify hazard areas and to some extent also hazard probabilities. In addition, considerable attention was given to problems of the "second collision" and much work was devoted to identifying the contributing factors involved in accident severity*, using FARS and injury severity data taken from the NCSS study.

4.4.2 Identification/Development of Safety Programs

The "system safety" approach to highway safety program development has always been complicated by the conflicting demands of accident prevention and accident protection and by philosophical differences between those who believe in the merits of highway or vehicle-related engineering or technological solutions to accident prevention and protection and those who favour more behaviour-oriented approaches to achieving these same goals.

In the first place, the natural orientation of highway engineers does not automatically lead to a "system safety" emphasis on accident prevention (as it would for example at NASA). In fact, the lack of system control in the highway mode, particularly with respect to the all-important human element, tends to divert engineering attention to the task of protecting vehicle occupants by controlling the effects of the "second collision" through a better understanding of vehicle dynamics, vehicle occupant kinematics and the structural properties of vehicles and guardrails.

---

* A.C. Malliaris et al. "A Search for Priorities in Crash Protection". In Society of Automotive Engineers. Crash Protection SP-J13; Proceedings of the International Congress and Exhibition. Detroit: Author, February 22-26, 1982.

Paradoxically, it is the behaviourial scientists at the NHTSA who tend to take the accident prevention route by giving emphasis to driver education, public awareness campaigns (including alcohol-related programs) and strict enforcement of highway regulations. The resulting program mix may be described as a compromise between these two contrasting safety management approaches.

The identification and development of appropriate accident prevention and protection countermeasures always tends to be the most complex and controversal stage of the planning process. In the present instance, the process itself was both formal and informal and involved synthesis of the Agency's on-going data analysis, modelling and research and development activities.

4.4.3 Program Selection and Prioritization

The selection, prioritization and organization of safety improvements in the form of the final Priority Plan was also the result of both formal and informal management process. However, three major decision criteria were identified to assist management in this regard. They were:

- magnitude of the safety problem;
- potential safety benefits;
- consideration of costs.

In the first place, it was considered sound policy to give priority to the most serious problem areas, and to the most intractable contributing factors in a particular problem situation. However, this was clearly unrealistic without giving attention to the probability and cost of success in implementating the program under evaluation. In addition, it was recognized that the Agency could not ignore the multitude of smaller safety issues which continually arise.

In the second place, the fact that accidents invariably embody a number of contributing factors means that there will normally exist at least an equivalent number of points at which safety improvements could possibly be made either to avoid or mitigate the consequences of accidents. These were all evaluated in terms of their potential benefits, including ease of implementation and timing.

Finally, consideration was given to the potential costs of an improvement. However, "cost" was treated in the broad sense to include such intangibles as personal sacrifice, lost opportunities or reduced expectations. Safety could be dramatically improved for example, by limiting nightime driving or by further lowering maximum speeds. Such measures would likely be impractical however, since the costs would far outweigh the potential benefits in the eyes of the driving public (or the politician).

In summary, the NHTSA methodology embodied a broad range of activities, including statistical analysis and mathematical modelling techniques, but in the main, the basis of decision was judgemental and was developed both formally and informally in management meetings and committees. This approach was a conscious one on the part of the Agency which has long held for example that formal benefit/cost analysis techniques, while helpful in certain specific situations, can never be a substitute for the informed judgement of policy makers and program planners.

4.5 Federal Highways Administration Rational Determination of Priority Targets for Research and Development

The FHWA asked Stanford Research Institute to develop a rational method of establishing research and development priorities. Completed in December 1976, this study consists of two reports and two volumes of working papers as follows:

- Interim Report for Task A: Highway Research Goals, Organizations and Decision Processes, September 1973;

- Rational Determination of Priority Targets for Research and Development: Summary Guidelines for Establishing R&D Priorities at FHWA, December 1976;

- Working Paper Volume I. Application of Decision Analysis to FHWA R&D Planning, September 1974;

- Working Paper Volume II. FHWA R&D Planning and Project Analysis, September 1974.

This study is the only one of the six studies reviewed in this section which has as its primary objective the establishment of a methodology to assist management planning of the R&D function. However, the FHWA objective differs from the objective pursued by TDC in two important respects. In the first place the method is designed to support management of the total R&D program function of the FHWA, not just the safety R&D function. Secondly, the methodology is not designed to assist in establishing R&D needs, but to establish R&D priorities. In effect, it takes the needs as given and focusses rather on the R&D project selection process (i.e., the third phase of the planning process). Some analysis of individual problem areas (e.g. safety, congestion etc.) is conducted in order to generate candidate R&D projects for each area, but the thrust of the method is to assist management in the task of prioritizing projects already identified.

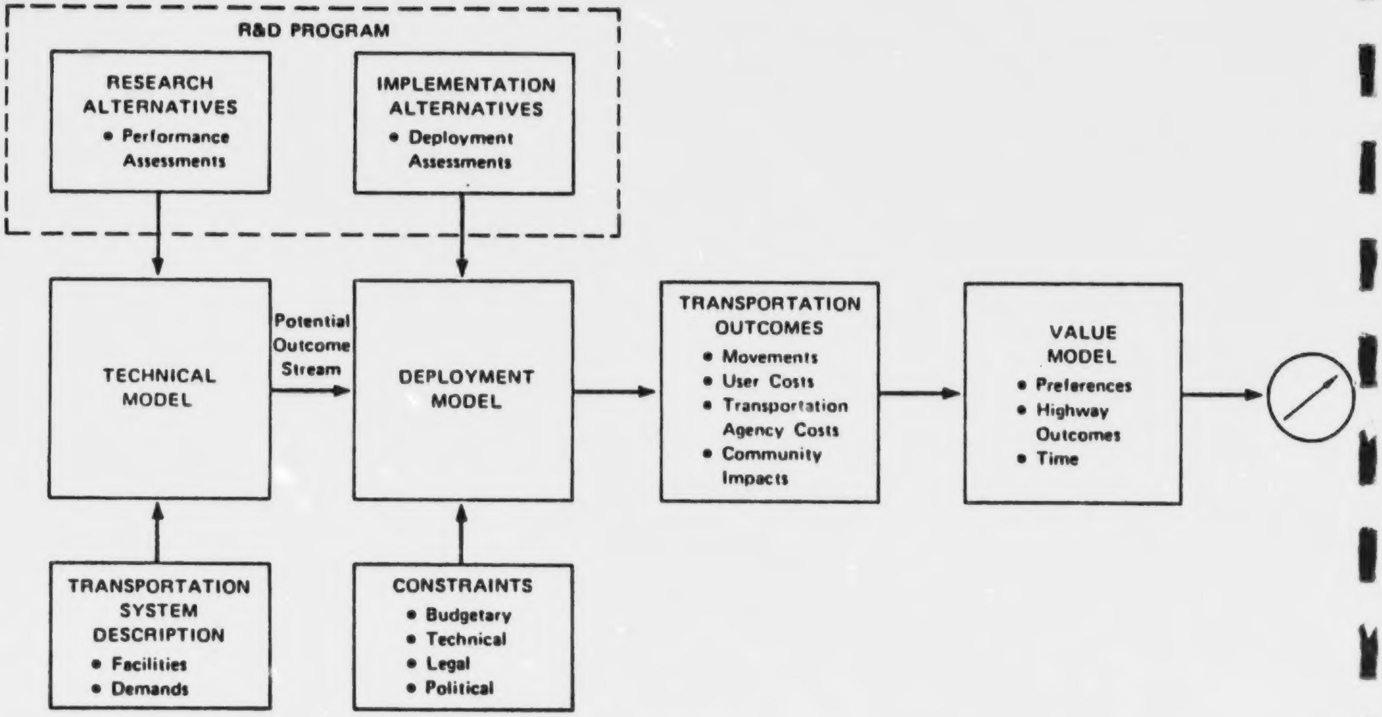
The four major problem areas reviewed in this study are the following:

- safety;
- congestion;
- construction and maintenance;
- socioeconomic and environmental.

However, in the development of the basic decision analysis methodology, SRI did focus its efforts in the area of highway safety R&D prioritization.

EXHIBIT 4.3

FRAMEWORK FOR HIGHWAY R&D EVALUATION


R&D PROGRAM
RESEARCH ALTERNATIVES
• Performance Assessments
IMPLEMENTATION ALTERNATIVES
• Deployment Assessments
TECHNICAL MODEL
Potential Outcome Stream
DEPLOYMENT MODEL
TRANSPORTATION OUTCOMES
• Movements
• User Costs
• Transportation Agency Costs
• Community Impacts
VALUE MODEL
• Preferences
• Highway Outcomes
• Time
TRANSPORTATION SYSTEM DESCRIPTION
• Facilities
• Demands
CONSTRAINTS
• Budgetary
• Technical
• Legal
• Political

Source: Stanford Research Institute.
Rational Determination of Priority Targets for Research and Development.
Prepared for the U.S. Federal Highway Administration, December 1976.

The effectiveness of the method was subsequently tested by applying the method, first in the safety area and then in the other three main areas of concern.

4.5.1 Description of Methodology

The method is designed to measure the economic impact of R&D project deployment in terms of so called "outcome variables". These include the actual R&D outputs, the effects of R&D deployment, and various transportation costs and benefits such as safety impacts (accidents, fatalities, injuries etc.); effects on travel time, comfort, convenience and user "anxiety"; effects on vehicle capital and operating costs; effects on the transportation system itself (construction, operating and maintenance costs); and finally community effects in terms of social, economic and environmental factors.

The basic evaluation structure shown in Exhibit 4.3 opposite is essentially a method of relating decision inputs (described as "modelling variables") to these benefit and cost outputs (i.e., the R&D and other "outcome variables").

These decision inputs are essentially of three kinds. Decisions may be made regarding the actual R&D alternatives chosen (e.g. differences in physical hardware or software design), regarding the manner in which these alternatives are deployed (i.e, implemented) and regarding the transportation system and the causal variables chosen for measuring eventual transportation system changes (e.g. "outcome variables" such as reduction in accidents, fatalities, etc.).

In this manner performance and deployment assessments are made of the various R&D research and implementation alternatives (the "R&D Program") and results quantified as far as possible, in terms of the potential changes in transportation outcomes ("outcome variables"). These tasks are performed by means of informed judgement or by more structured methods.

Results are translated into social costs and benefits by means of a so-called "value model". This is simply the assignement of dollar "value" units to such things as e.g. fatalities, injuries or property damage, based on information culled from a variety of sources (special studies etc.).

Final assessments and analyses are presented in the form of a project portfolio listing the net social value of the various "outcome variables". A "portfolio selection" technique is used to select a subset of total projects such that the net social benefits are maximized and total costs of research, development and implementation of the R&D package do not exceed the total budget. When R&D project outcomes are independent of one another, the portfolio problem is the well-known knapsack problem. However, when projects are interdependent with respect to their expected outcomes, the solution is somewhat more complex since the benefits of a set of projects are not necessarily equal to the sum of the benefits of the individual projects in the set.

Three approaches were used to solve this problem, branch and bound, integer programming formulation and the gradient approach. An algorithm based on the gradient approach was found to be simpler and the easiest practical solution.

Throughout the analysis, probability distributions may be substituted in cases of uncertainty regarding the exact parameters of important variables. In this manner, the decision process could pass through an iterative cycle leading from the "deterministic" phase to a "probabilistic" phase and on to a further "informational" phase where the merits of gathering new and better sources of management information are evaluated.

The SRI "method" is essentially a management framework for decision-making which employs a portfolio management approach to the R&D selection and prioritization process. It was successfully demonstrated but never subsequently implemented at the FHWA. In view of its general scope and orientation it may be considered to be only marginally relevant to the present research effort. Its principal strength is that it is able to establish R&D priorities for a diverse group of projects in many different areas simultaneously. However, it suffers from being overly complex and conceptually fuzzy in certain respects.

4.6 Federal Railroad Administration Track Rehabilitation and Maintenance Research Requirements

The FRA administers and enforces Federal laws and regulations designed to promote safety in railway transport and exercises jurisdiction over all areas of rail safety such as track maintenance and inspection standards and equipment standards. In addition, this Agency is required by the Railroad Safety Authorization Act of 1980 to submit an annual "System Safety Plan" to Congress. The first such document, published in December 1981, identified major goals and developed a program of safety priorities in the areas of track, equipment, operating practices, signal and train control and hazardous materials transportation. The plan established a priority order for concentrating safety efforts on accident categories that pose the highest risk of fatalities, injuries and property damage. The 5-year objective is to reduce by 20% accidents in the following categories:

- hazardous materials releases;
- serious passenger train accidents;
- railroad employee casualties;
- rail-highway crossing accidents;
- trespasser fatalities.

Research and development is an essential component in the search for means to accomplish the above program goals. In the two main areas of track and equipment rehabilitation and maintenance, major program areas include:

- Track Train Dynamics Program designed to determine how existing cars in the present fleet can be improved to be more stable when operating over poor track;

- Truck Design Optimization Program, designed to develop performance and test specifications for safe and more stable freight car trucks;

- The Locomotive Research and Train Handling Evaluator, a tool used to evaluate operating procedures and control devices to ensure that long trains can be operated as safe as short trains;

- Various other test programs at the Facility for Accelerated Service Testing and at the Rail Dynamics Laboratory.

In addition, the FRA is involved in programs of research on metallurgy, thermal insulation, safety valves to improve the transport of hazardous materials, studies regarding the routing of nuclear wastes, of spent nuclear fuel casks and the rerouting of hazardous materials away from major population centres.

4.6.1 Establishment of R&D Requirements

The establishment of these R&D program requirements is a complex undertaking which involves a coordinated process of exchange of information and inputs from the railway industry. The Office of Research and Development of the FRA commissioned three studies in an attempt to identify R&D needs in the areas of track and bridge rehabilitation and maintenance. These were as follows:

- The MITRE Corporation. Track Rehabilitation and Maintenance Research Requirements. Washington DC, Federal Railroad Administration FRA/ORD 80/09, January 1980.

- The MITRE Corporation. Track Rehabilitation Research Requirements: A Basis for Program Planning. Washington DC, Federal Railroad Administration FRA/ORD 80/10, March 1980.

- Parsons, Brinckerhoff, Quade, and Douglas, Inc. Track and Bridge Maintenance Research Requirements. Washington DC, Federal Railraod Administration FRA/ORD 80/11, March 1980.

The first of these studies represents a synthesis of the total work effort of both study teams. It should be noted that the objectives of this work were to identify alternative R&D thrusts aimed at improving the cost-effective performance of the track structure in terms of track rehabilitation and maintenance. It was not aimed at safety aspects or at matters not related to track such as equipment. It was felt however, that the methodology developed in these studies might also find some application in safety-related R&D program development.

The approach taken in these studies was similiar to that adopted in similar studies undertaken for/by other DOT agencies, viz:

- problem identification/definition;
- program/subprogram development;
- program/subprogram selection and prioritization.

4.6.2 Problem Identification/Definition

A rank ordering of track rehabilitation and track maintenance problems was established in each case by means of:

- preliminary list of track system problems established on the basis of interviews, literature reviews and previous survey results;

- classification of problem areas by track system components according to whether they concerned:

  - inadequate materials,
  - inadequate methods,
  - insufficient information;

- face-to-face review with government, contractor and industry representatives who were asked to rank-order problem areas;

- synthesis of interview findings.

4.6.3 Program/Subprogram Development

For each of the two main R&D programs (track rehabilitation and track maintenance), a number of individual R&D subprograms were developed, corresponding to the main problem areas already identified. This was accomplished by descending order of track problem area. The information required to design each subprogram was taken from four sources:

- face-to-face interviews;
- literature reviews;
- telephone interviews;
- experience of the study team.

It was quickly noted that a subprogram designed to solve one problem could also affect other problem areas. For example solving the problem of excessive rail wear through improved rail metallurgy also goes a long way towards solving the problem of premature rail failure and excessive rail corrugation. In the track rehabilitation area it was found that 13 subprograms related to the top 30 program areas.

4.6.4 Program/Subprogram Selection and Prioritization

The selection and prioritization of R&D subprogram elements was accomplished by the study teams on the basis of the following evaluation criteria:

Criterion	Description	Weight
Benefit-Cost Ratio	Present value of net dollar benefit to RR industry divided by R&D cost	0.40
Safety Impact	Number of accidents prevented in first 5 years of implementation	0.15
Capital Savings	Capital expenditures saved in first 5 years of implementation	0.16
Timeliness	R&D time in years	0.12
Other Impacts	Subjectively selected value from a scale of -5 to +5	0.09
R&D Cost	Total subprogram R&D cost	0.07

In order to provide an overall score for purposes of rank-ordering the priorities, each criterion was assigned a weighting value and each program was also evaluated in terms of its probability of success. In this manner, the risk element associated with successful achievment of R&D objectives was also incorporated into the analysis. The result was a rank-ordering of R&D subprogram elements, based largely on judgemental estimates guided by certain pre-established criteria.

This R&D Program Plan was not fully implemented at the FRA due to changes in program priorities as a result of subsequent political developments.

4.7 Urban Mass Transportation Administration Safety Program Plan

The Urban Mass Transportation Administration (UMTA) is one of two DOT Agencies which has adopted a "system safety" approach to safety program or project planning. In providing funding assistance to states and local governments for purposes of developing and constructing urban mass transit systems, the UMTA has considerable leverage in the safety area. For example, transit authorities are required to develop and implement a System Safety Plan (SSP), based on guidelines developed for the Agency as a result of studies by Batelle Columbus Laboratories*. When the UMTA Office of Safety and Product Qualification (OSPQ) was established in July 1976, the Agency called upon the Institute of Safety and Systems Management of the University of Southern California to assist them in developing a Safety Program Plan for this Office**.

The study is unique in recognizing and building on the premiss that the activities of any agency should be related to a hierarchy of explicit mission objectives and goals. In this manner, the "problems" to be addressed are completely determined and defined in terms of the prescribed objectives of the Agency rather than the other way around. Program need becomes completely mission-dependent and the Safety Program Plan is developed from the ground up through a consideration of the goals and objectives of the DOT, of the UMTA and of the Associate Administrator for Technology Development and Deployment to which the OSPQ was organizationally attached.

This kind of policy analysis resulted in a set of six key objectives for the Office. Following these, twenty nine critical objectives and over ninety specific objectives were defined and recommended as necessary steps to the accomplishment of the key objectives. The key objectives recommended for consideration by the UMTA management were as follows:

1. decrease accident rates;
2. eliminate catastrophic accident conditions;

---

* E.S. Cheany et al. Safety in Urban Transportation: Guidelines Manual. Columbus: Batelle Columbus Laboratories, 1975. Prepared for the U.S. Department of Transportation, Urban Mass Transportation Administration, UMTA-RI-06-0005-75-3.

** G.P. Jones et al. Development of a Safety Program Plan for the Office of Safety and Product Qualification. Los Angeles: Institute of Safety and Systems Management, University of Southern California, September 1977. Prepared for the U.S. Department of Transportation, Urban Mass Transportation Administration. NTIS PB 279-331/332.

3. prevent "unsafe" conditions;
4. assure use of "best" technology;
5. accomplish objectives in a cost-effective manner;
6. determine and correct "unsafe" conditions.

These objectives and the various sub-objectives identified along with them, provided the rationale for the identification and selection of the sixteen specific safety programs which were recommended to form the skeleton of the Safety Program Plan as such.

Of particular interest from the point of view of the present study, is the work conducted with respect to the development of programs related to the first and principal objective defined for the OSPQ, viz: decrease accident rates. The critical objectives defined for this key objective were as follows:

1a. collect and analyze accident data;
1b. collect and analyze transit volume data;
1c. define problems and potential solutions;
1d. develop potential solutions;
1e. implement resulting solutions;
1f. evaluate results.

The further breakdown into specific objectives is shown in Exhibit 4.4 opposite. In this manner, the key objective (which determines and defines the need) is translated into the actual tasks which together constitute both a framework and method for developing specific programs (in this case to decrease accident rates).

4.7.1 Identification of Problem Areas

While the identification of safety problems is specifically related to critical objective 1c. above, the collection and analysis of accident and transit volume data is also emphasized as key to the development of the system safety methods required. In this connection, a safety "problem area" is considered synonymous with a "hazard area" and the method thus involves the identification and (where possible) the quantification of safety hazards, defined as "a potential source of loss".

The study presents a general approach to the identification and quantification of hazards. Actual loss in terms of death, injury or property damage will depend not only on the existence of hazards but also on exposure to them and on the relation of the exposed agent to these hazards, i.e., his/her vulnerability (cf. Exhibit 4.5 overleaf). Vulnerability will influence loss though the degree of accident severity.

The study also develops a set of principles or criteria for the development of a viable hazard identification methodology. Thus, the method:

- must provide for current and future systems;

EXHIBIT 4.4

UMTA/OSPQ PROGRAM PLAN STUDY
CRITICAL AND SPECIFIC OBJECTIVES FOR KEY OBJECTIVE NO. 1

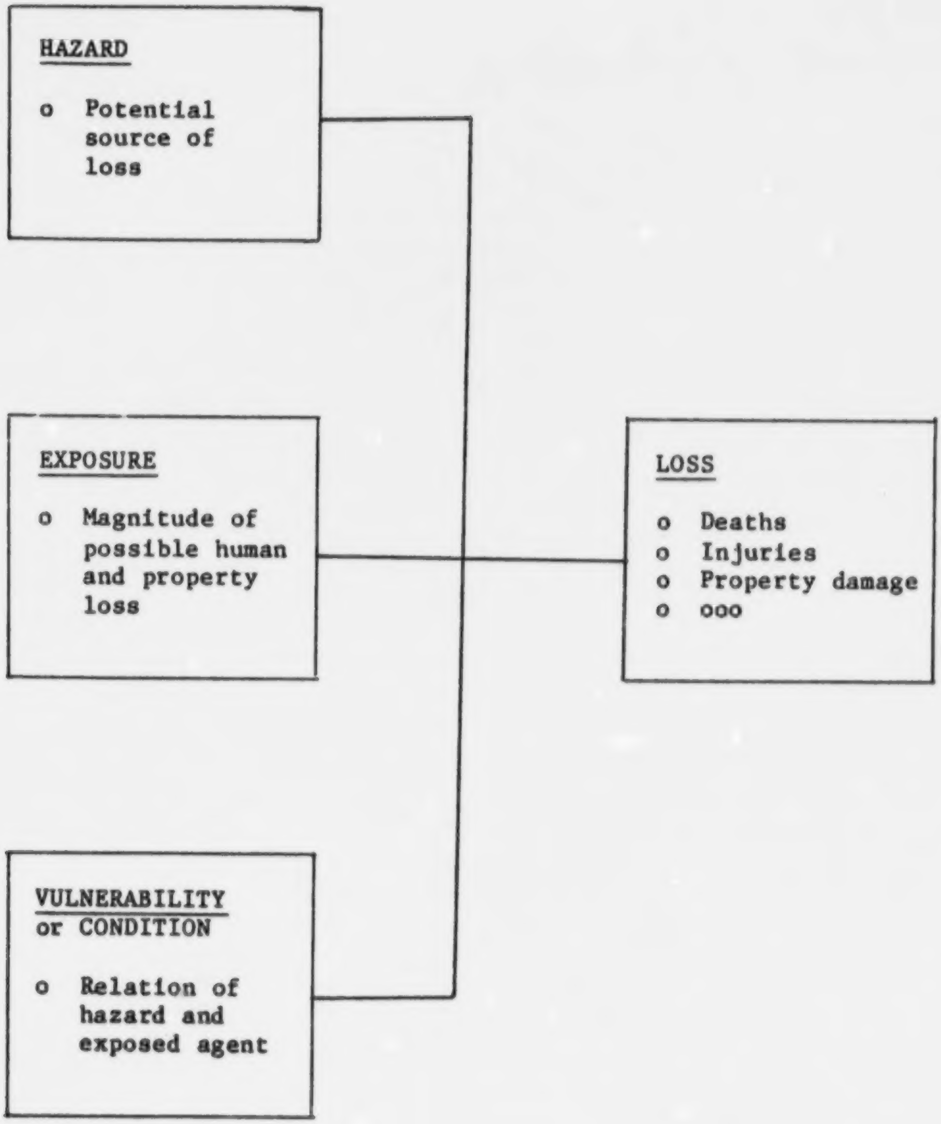
Key Objectives
  Critical Objectives
    Specific Objectives

1. Decrease Accident Rates
   - 1.A Collect and Analyse Accident Data
     - 1.A.1 Determine Required Results
     - 1.A.2 Determine Input Requirements and Format
     - 1.A.3 Coordinate with Associated Agencies
     - 1.A.4 Coordinate with UMTA Grant Provisions
     - 1.A.5 Coordinate Data Reduction Program
   - 1.B Collect and Analyse Transit Volume Data
     - 1.B.1 Determine Required Results
     - 1.B.2 Determine Input Requirements and Format
     - 1.B.3 Coordinate with Associated Agencies
     - 1.B.4 Coordinate with UMTA Grant Provisions
     - 1.B.5 Coordinate Data Reduction Programs
   - 1.C Define Programs and Potential Solutions
     - 1.C.1 Analyze Accident and Rate Data
     - 1.C.2 Determine Important Hazard Areas
     - 1.C.3 Review Past and Present Efforts
     - 1.C.4 Determine Areas for Expanded Effort
     - 1.C.5 Define and Evaluate Potential Solutions
   - 1.D Develop Potential Solutions
     - 1.D.1 Detail Problem
     - 1.D.2 Develop and Evaluate Alternative Solutions
     - 1.D.3 Develop Specific Selected Alternatives
   - 1.E Implement Resulting Solutions
     - 1.E.1 Coordinate UMTA Grant Provisions
     - 1.E.2 Coordinate Regulatory Measures
     - 1.E.3 Encourage Use of "Best" Technology (Key Objective No. 3)
   - 1.F Evaluate Results
     - 1.F.1 Analyse Data on Accidents and Rates
     - 1.F.2 Conduct Specific Analyses
     - 1.F.3 Document Measured Results

Source: University of Southern California.
Institute of Safety and Systems Management.

EXHIBIT 4.5

HAZARD IDENTIFICATION AND EVALUATION PROCESS


HAZARD
o Potential source of loss
EXPOSURE
o Magnitude of possible human and property loss
VULNERABILITY or CONDITION
o Relation of hazard and exposed agent
LOSS
o Deaths
o Injuries
o Property damage
o ooo

Source: University of Southern California. Institute of Safety and Systems Management.

- must be compatible with current/future data collection systems;

- must include all major casualty producing situations;

- must be broad in nature but with ability to develop a consistent hierarchical structure for each specific hazard;

- must provide a fruitful analytic framework;

- should provide for multimodal transference and cross modal analysis where possible;

- should be compatible or provide cross reference to OST program element structure.

The major difficulty reported by the authors of the study was the fact that none of the existing or potential sources of accident, loss or exposure data were adequate to the task at hand. Data collection systems all tended to be specific to a given organization or purpose, were descriptive rather than causal and did not exhibit the common comparative measures necessary for making comparisons across the different modes within the transit field. This fact alone prompted the establishment of two program areas:

- define and implement accident data banks;
- define and implement transit volume data banks.

In the interim, however, the study was able to identify (though not to quantify) major hazard areas on the basis of analysis of data summaries developed from the Federal Railroad Administration (FRA) Railroad Accident/Incident Reporting System (FRAIRS) in conjunction with studies undertaken by Mateyka and Talley*.

The major hazard areas are shown in Exhibit 4.6 overleaf. The actual ratings were largely arrived at judgementally, based on the statistics and on the result of an extensive literature search (Appendix D of the study).

Ideally, however, the study recommended that transit hazard identification be based on analyses of transit accidents in terms of a threefold typology of the accident process as follows:

TriggeringEvent	System Malfunction	Accident Event
1. Material failure	1. Vehicle (component)	1. Collision
2. Mfg./Const. defect	2. Signal/comm. (component)	w/system vehicle
3. Improper operating	3. Propulsion (component)	w/non-system vehicle
procedure	4. Station/platform	w/ pedestrian
4. Human failure	ADD FOR RAIL	w/fixed object
5. Natural forces	5. Track	2. Fire/explosion
6. Non-system activity	Note: there may be no	3. Release of toxic agent
7. System Design inadequacy	system failure and a trig-	4. Personal causal
	gering event may directly	ADD FOR RAIL
	result in an accident event	5. Derailment

---

* J.A. Mateyka and H. Talley. "System Safety/Risk Analysis Techniques Applied to Motor Vehicles and Rapid Transit Systems*. Journal of Safety Research Volume 9, No. 1, March 1977, pp 2-14.

EXHIBIT 4.6

UMTA/OSPQ SAFETY PROGRAM PLAN STUDY RAIL HAZARD AREA RATINGS

	Based on FRA Rapid Rail Transit Data		Based on Booze, Allen Applied Research (33)			Importance Classification
Hazard Area	Injuries	Fatalities	Frequency	Hazard Index	Criticality Index	High Medium Low
1 In Station	1*	2	1*	Major to Critical	2	High
2 On Trains in Normal Operations	2	3	4	Major to Critical	5	Medium
3 Boarding and Alighting	3	4	3	Marginal	6	Medium
4 On the Right of Way		1*	2	Critical	1	High
5 Derailments			5	Catastrophic	3	Low
6 Collision with Vehicle on Guideway			6	Catastrophic	4	Low

* = High group

Source: University of Southern California.
Institute of Safety and Systems Management.

EXHIBIT 4.7

UMTA/OSPQ SAFETY PROGRAM PLAN STUDY

RAIL RAPID TRANSIT--PEOPLE EXTERIOR TO TRAIN--ACCIDENT SCENARIO

	BEFORE	DURING	AFTER
Potential or Existing Passengers	-- Entering station -- In corridors, pay stations, etc. -- On stairs or escalators or elevators or ramps -- On platform	-- Slips on debris, ice, snow, wet surfaces -- Walk or run into obstructions -- Fall on "poor" surfaces -- Fall on stairs or escalators -- Hit by approaching train sides	-- Reports accidents to attendant if able or reported by others
Vehicle	-- Vehicle entering station or proceeding along right of way -- Escalators, elevators and stairs	-- Vehicle strikes person -- Person injured by fixed or moving objects or subjects in station	-- If aware of the accident the vehicle stops or the escalators or elevators are stopped
Environment	1) Bad weather may increase surface hazard & cause people to wear cumbersome footware & clothing 2) Dirty & cluttered stations and platforms 3) Train entering station causes heightened tension 4) Crowded conditions may cause pushing 5) Architectural design may be hazard	-- Accident causes commotion, especially if serious additional milling and pushing may occur. Tension is greatly increased	-- People worried about delays -- Some may want to leave station -- Confusion & concern are heightened -- If trains are delayed crowds may begin to jam-up. People in other delayed trains are apprehensive
Management and procedures	-- Normal operation, little or no crowd control -- Periodic cleaning operations -- Limited repair or upkeep services	-- Normal operations	-- Receive accident reports -- Notify proper agencies for services -- Provide first aid -- Provide access in stations -- Re-schedule as required -- Follow-up claims

Source: University of Southern California.
Institute of Safety and Systems Management.

The term "triggering event" is preferred to the word "cause" due to the multiplicity of events normally involved in a given accident situation. These events may or may not result in a malfunction or failure of part of the system, depending on inherent internal system recovery capabilities such as fail-safe mechanisms. The accident event itself may, of course, be classified in a number of ways, depending on the type and degree of detail required.

There are a total of 210 basic event categories in the above classification (7x6x5 independent possibilities, including that of "no system malfunction"). Since this is too detailed for program planning purposes, the study recommends reducing the total to 10-20 of the most serious and relevant basic event categories by applying some judgement to the analysis process.

4.7.2 Identification/Development of Safety Programs

Following the definition of hazard areas, attention is directed to identifying cost-effective countermeasures or programs designed to mitigate the problem. Two approaches were considered:

- refine problem areas to higher levels of resolution;
- develop scenarios of accident type.

The first approach was the one adopted by the U.S. Coast Guard Study described in the following sub-section of this report. However, this was impractical for UMTA/OSPQ on the basis of the available data and it was therefore decided to opt for the second approach. Exhibit 4.7 provides details of the scenario developed for persons involved in accidents taking place in areas other than in the railcars themselves. These scenarios were all developed judgementally, based on the expert knowledge of study team members.

Individual scenarios formed the basis for the identification and development of a range of accident countermeasures as illustrated in Exhibit 4.8. The evaluation/prioritization and selection of countermeasures in terms of individual program and project elements was accomplished judgementally on the basis of expert knowledge and opinion, and justified back to the original key and critical objectives of the Agency and of the Office of Safety and Product Qualification. This process was formalized to a certain extent by means of "Program Justification" Forms.

It should be noted that the Program itself does not suffice to select and prioritize individual projects. It is in effect the objective and task of the Program itself to "detail and evalute the implications of countermeasures ...". No specific methodology is proposed to accomplish this. The deliverables thus include:

- detailed solution alternatives;
- evaluation of each alternative;
- proposed specific programs for development.

EXHIBIT 4.8

UMTA/OSPQ SAFETY PROGRAM PLAN STUDY

RAIL RAPID TRANSIT--PEOPLE EXTERIOR TO TRAIN--ACCIDENT COUNTERMEASURES AND MITIGATIONS

	BEFORE	DURING	AFTER
Potential or Existing Passengers	1) Provide assists and directions to use 2) provide clear directions and transit information to reduce tension and confusion 3) Provide information for "what to do in case of ..."		
Vehicle, Track & Station	1) Snow, ice, rain and debris removal inside and outside station 2) Uncluttered passage ways and platforms 3) Isolation of people from platform edge and track way 4) Well lighted and well designed station 5) Proper lighting of track ways 6) Edge--treatment of platform 7) Reduce "vertical transit" hazard	1) Eliminate exposed 3rd rails 2) Provide "suicide pits" or niches 3) Provide "people catchers" on train 4) Eliminate between cars hazards 5) Keep stairs & escalators short, gradual, slow. Provide alternatives	1) Provide for extrication of injured from the equipment 2) Provide equipment for isolation of injured, and first aid 3) Provide immediate stopping of moving equipment involved 4) Provide for emergency service access to injured
Environment	1) Provide well designed, clean, uncluttered, bright, interesting environments in stations and platforms 2) Announce train entry and designation or destination		
Management and Procedures	1) Selection and training of motormen and attendants 2) Slow entry into stations by trains 3) Provide crowd control attendants 4) Identification procedures for potential suicides 5) Maintain facilities in "good" condition	1) Provide for immediate crowd control 2) Isolate injured if possible	1) Notify the people and calm them 2) Provide people with information on probable outcome and alternate actions if appropriate

Source: University of Southern California.
Institute of Safety and Systems Management.

For these reasons, the UMTA/OSPQ Safety Program Plan methodology is not as detailed or as comprehensive as that developed in connection with the U.S. Coast Guard RDT&E Plan described below.

4.8 U.S. Coast Guard Research Development, Testing and Evaluation Plan for Marine Safety

A more detailed "system safety" approach to assisting management in the establishment of research and development needs was developed by the Batelle Columbus Laboratories in conjunction with work undertaken for the U.S. Coast Guard. As a result of increased research, development, testing and evaluation (RDT&E) needs in support of various safety mission activities of this Agency, Batelle and the Coast Guard Office of Research and Development developed a "RDT&E Plan for Marine Safety", completed in May 1977*. This comprehensive plan was designed to support all programs within the marine safety domain of Coast Guard "M" and "W" Offices of Merchant Marine Safety and Marine Environment and Systems respectively**. These programs included:

- Commercial Vessel Safety Program;
- Aids to Navigation Program;
- Bridge Administration Program;
- Marine Environmental Protection Program;
- Port Safety and Security Program;
- Deepwater Ports Project;
- Ports and Waterways Planning.

The term "marine safety" was broadly defined to include freedom from occurances hazardous to:

- life and well-being of people;
- property;
- the marine environment.

The marine domain was taken to include vessels, personnel, facilities and other property both onshore and offshore, cargo, passengers, the waterways, and all commercial (including offshore oil, gas, and mining) and recreational activities carried out in the oceans and island waterways of concern to the Coast Guard.

It was recognized that the Plan could only be developed in the light of a full understanding of the nature and purposes of the mission activities it was intended to support. However, these activities fell into a number of categories, some of which did not have safety as the only recognized goal. (This is of course another illustration of the universal problem already discussed in section 1.3.3 of this report.) In this connection, the study objective was to design a RDT&E Plan "... to support all activities concerned with marine safety and environmental protection", but to include a companion "all other" goal category as a means of collecting RDT&E items supporting other non-safety-related activities. It is important to note that RDT&E at the Coast Guard is treated as a support activity conducted in support of Coast Guard Programs.

---

* E.S. Cheany, R.D. Leis and A.J. Coyle. RDT&E Plan for Marine Safety. Columbus, Ohio: Authors, May 1977. Prepared for the U.S. Coast Guard, Office of Research and Development by Batelle Columbus Laboratories.

** However, the Plan was not in any way intended to recognize which organizational element of the Coast Guard might eventually be selected to be responsible for executing any part of the Plan.

The Coast Guard adopted a building block approach with respect to the development of a methodology to assist in establishing safety R&D needs. In this respect, the criterion of need is defined in terms of problem "seriousness" which is revealed through a two-step process as follows:

- identify safety problem areas by means of logic diagrams;
- determine problem "seriousness" in terms of the "expected loss" in allowing the problem to go unresolved.

Unfortunately, there are a number of difficulties inherent in the concept of "expected loss". In the first place it must be asked loss from whose point of view; the Agency, the transportation mode involved, society etc.? In the case of the Coast Guard, the expected loss was evaluated from the point of view of the Coast Guard (which presumably reflects the interests of society). In the second place, it is difficult to find a common yardstick by which to measure and evaluate losses of an intangible nature which defy a satisfactory quantitative analysis. Finally, and perhaps most importantly, the expected loss is a function of the risks involved in allowing a potential problem or hazard to remain. This suggests the need for some quantitative predictive tool to identify the conditional probabilities of accidents occurring in the various problem/hazard areas and the severity of their occurrence.

The Coast Guard therefore proposed to build up a body of data sources and methods on a step-by-step basis as follows:

- Forecast Major Transportation Trends:
    - vessel technology;
    - traffic patterns;
    - commodities;
    - siting of facilities.
- Establish Marine Safety History Information System (MSIS):
    - determine user needs;
    - establish data base and processing capabilities;
    - perform casualty investigation/analysis.
- Develop Micro-Statistical - Based Risk Analysis Method:
    - expand spill risk model;
    - expand vulnerability model;
    - standardize cost/benefit analysis of safety actions;
    - adopt general model to locality, river and coastal areas.

- Develop Macro-Statistical - Based Risk Analysis Method:
  - develop macro-economic profile of the marine domain;
  - develop low-resolution risk management techniques;
  - demonstrate methodology.

Collectively, these tasks are given top priority as primary problem area No. 1, called "problem analysis, definition and management information". They are all structured in terms of on-going work at the Coast Guard, particularly with respect to certain risk analysis methods which had already been developed for certain more specific purposes such as the prediction of spills and community vulnerability.

4.8.1 Planning Scope and Strategy

The scope of the RDT&E Plan went considerably beyond that undertaken on behalf of UMTA/OSPQ. The plan was designed to address the following major planning tasks:

- Identification of Marine Safety Problem Areas;
- Identification of Marine Safety RDT&E Project Areas;
- Identification of individual RDT&E Projects within Project Areas;
- Identification of specific Tasks for RDT&E Projects;
- Project Evaluation and Prioritization;
- Project Selection and Budgeting.

The main thrust of the work program was devoted to problem and project identification. The Plan did propose an approach to project evaluation and selection, but did not fully carry out these two important management tasks.

The strategy adopted by the planning team was somewhat different from that adopted by the UMTA/OSPQ study group. The UMTA/OSPQ study (having as its objective the design of a safety Program Plan) adopted the strategy of keying the development of Programs to a set of Agency and Office mission objectives defined by legislation and tradition. A lot of effort was therefore devoted to identifying these objectives and proceeding on the basis of successive breakdowns of goal statements. The Coast Guard study on the other hand, (having as its objective the design of a Safety RDT&E Plan for the support of Agency Programs) adopted the strategy of developing directed, alternative solutions to problems/subproblems defined in a hierarchical form from a single, all-embracing problem definition. In the words of the study; "In comparison to the other planning modes, problem solving appeared to provide the most direct response to the needs of the M/W activities; it has the tightest logic on which to rationalize the plan, and it seemed most commensurate with Coast Guard management's concept of the role RDT&E is expected to play in support of mission activities. The strategy of the study work program was therefore designed to, "generate a program of RDT&E projects/task whose results would solve the "RDT&E susceptible" problems hampering the Coast Guard's ability to prevent, nullify, or mitigate the consequences of marine casualties in an effective, efficient manner".

In this planning mode, RDT&E projects are keyed directly to marine safety problems rather than indirectly through Mission Goals and Agency Programs (which must necessarily also address safety problems, among others).

Development of the hierarchical structure of problem definition and project response took the following general form.

Problem Marine hazards/accidents	Response RDT&E Activities
General Safety Problem	Safety Mission Activities of CG
Hazard/Risk Areas	CG Programs
Primary Problem Areas	RDT&E Project Areas
Subproblem Areas	RDT&E Projects and Tasks (Project Elements)

The General Safety Problem is the existence of marine hazards and the fact of marine accidents. This is the raison d'être of the Safety Mission activities of the M/W Offices of the Coast Guard. However, the General Safety problem may be broken down into individual Hazard/Risk areas from the point of view of the various parties-at-risk. The breakdown proposed in this study is shown in Exhibit 4.9 overleaf. The problem-oriented activities of the M/W Offices (i.e., including those related to the General Safety Problem) is first partitioned into the twin problems of Marine Safety (Marine Domain Casualty) and "Other". The Marine Safety Problem is then subjected to a first level breakdown into the various hazard/risk areas (cargo, vessel, etc.) The "Other" category is only included in order to accommodate activities having a problem orientation in which safety is either one of several goals or else a spin-off of R&D undertaken in the service of facilitation, efficiency, etc.

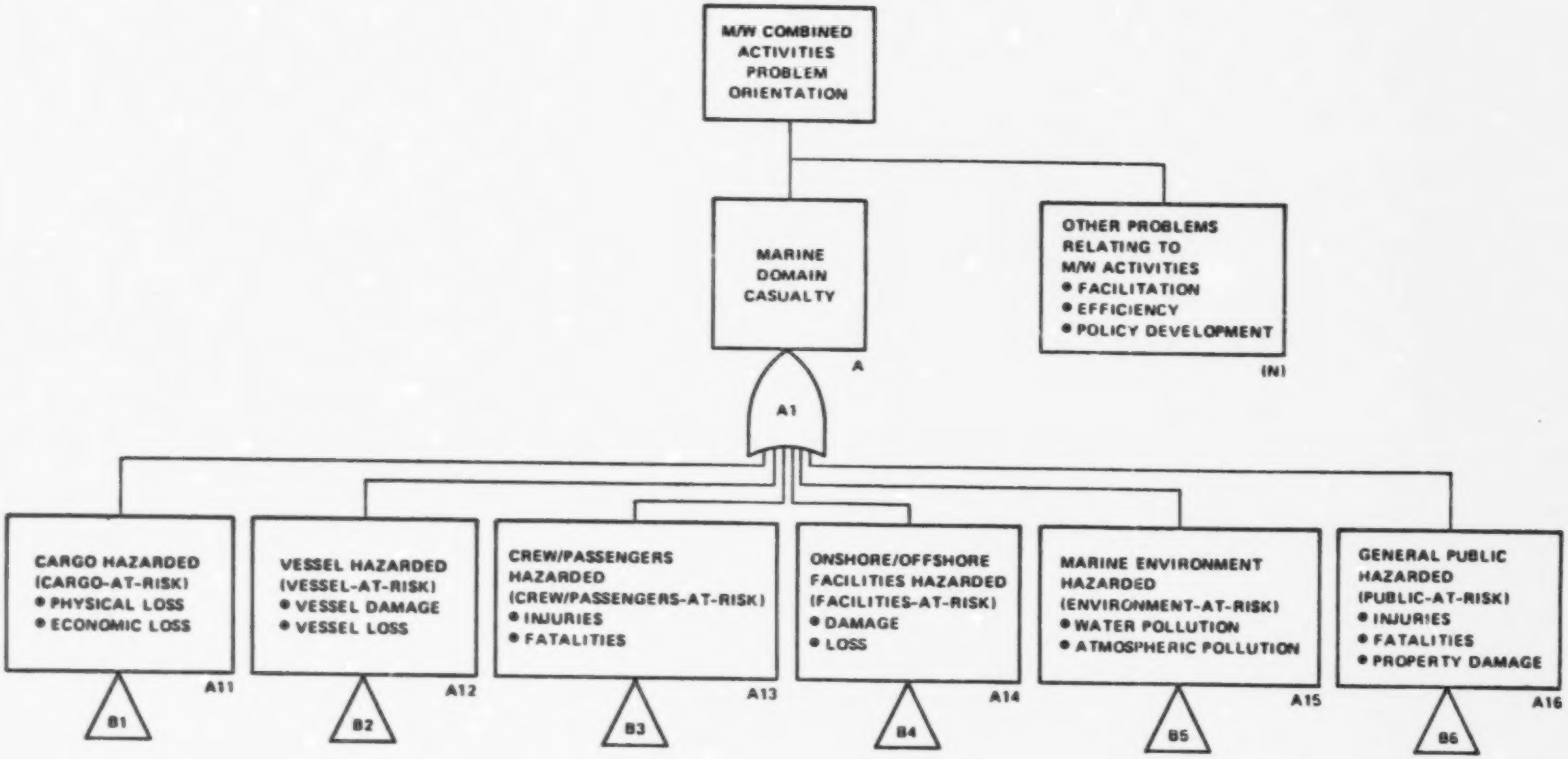
These hazard/risk areas are broken down in turn into fourteen Primary Problem Areas. The identification of Primary Problem Areas is key to the identification and development of equivalent responses or Project Areas which, as already mentioned, are the basic structural elements of the RDT&E Plan. The Primary Problem Area is a level of problem disaggregation (i.e., need establishment) sufficient to designate a unique, generic type of systemic failure or accident having two characteristics:

- it is equivalent to a marine domain casualty;
- it involves a single sector of technology within which a coherent set of hazard control actions (Project Areas) can be organized.

The conjunction of these two characteristics makes it possible to define the concrete response packages (Project Areas) in sufficient detail for their effectiveness to be assessed in terms of their potential for reducing or mitigating the occurence of the marine domain casualty problem involved, i.e., "to provide a measure of the safety improvements achievable through R&D". An example of a Primary Problem Area is "occurrence of fire/explosion". This is a generic type of accident occuring in vessels and facilities and it involves a definable technology. A coherent fire control activity can be organized and its effectiveness measured as a reduction in fire/explosion losses.

EXHIBIT 4.9

IDENTIFICATION OF PARTIES-AT-RISK


M/W COMBINED ACTIVITIES PROBLEM ORIENTATION
MARINE DOMAIN CASUALTY
A
A1
OTHER PROBLEMS RELATING TO M/W ACTIVITIES
• FACILITATION
• EFFICIENCY
• POLICY DEVELOPMENT
(N)
CARGO HAZARDED (CARGO-AT-RISK)
• PHYSICAL LOSS
• ECONOMIC LOSS
A11
B1
VESSEL HAZARDED (VESSEL-AT-RISK)
• VESSEL DAMAGE
• VESSEL LOSS
A12
B2
CREW/PASSENGERS HAZARDED (CREW/PASSENGERS-AT-RISK)
• INJURIES
• FATALITIES
A13
B3
ONSHORE/OFFSHORE FACILITIES HAZARDED (FACILITIES-AT-RISK)
• DAMAGE
• LOSS
A14
B4
MARINE ENVIRONMENT HAZARDED (ENVIRONMENT-AT-RISK)
• WATER POLLUTION
• ATMOSPHERIC POLLUTION
A15
B5
GENERAL PUBLIC HAZARDED (PUBLIC-AT-RISK)
• INJURIES
• FATALITIES
• PROPERTY DAMAGE
A16
B6

Source: Battelle Columbus Laboratories.

EXHIBIT 4.10

PRIMARY PROBLEM AREA LOGIC DIAGRAM

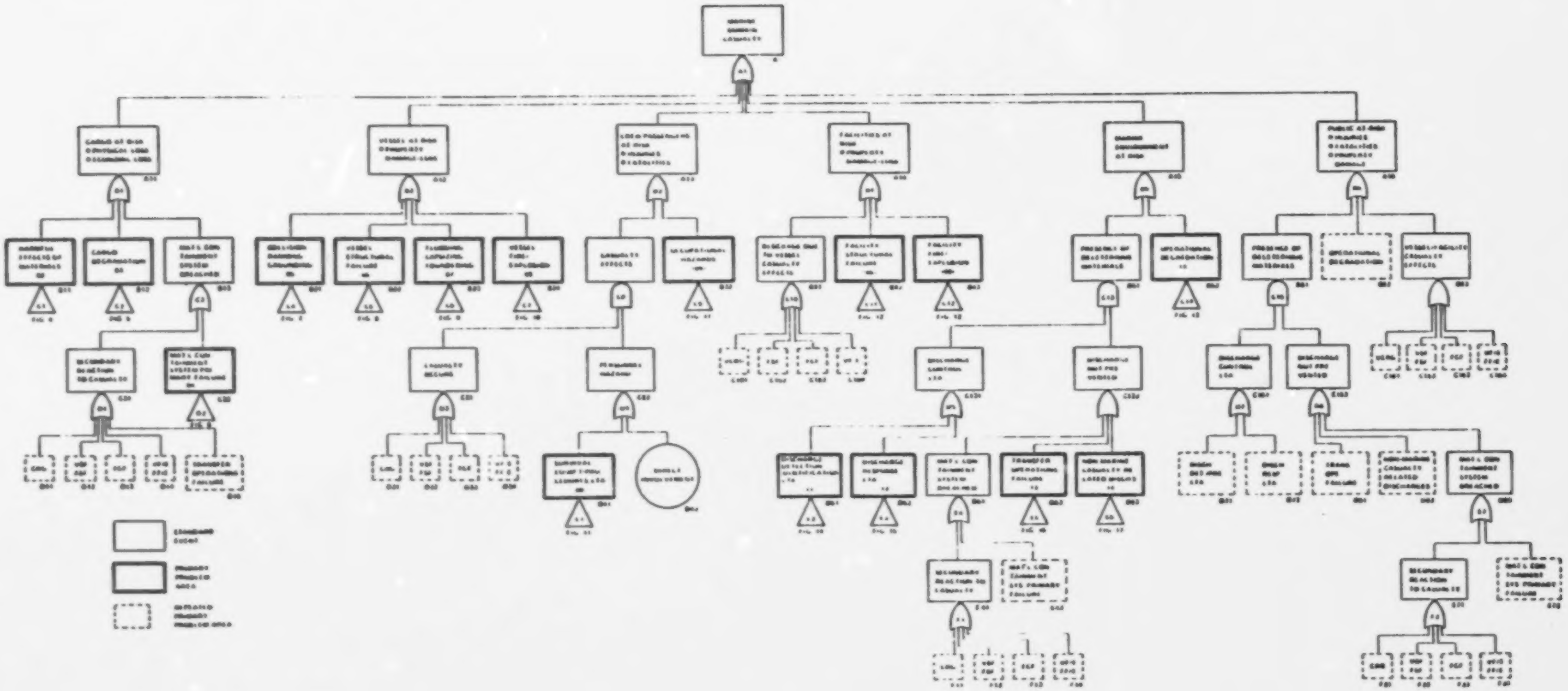
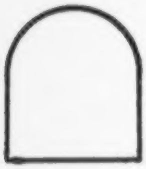
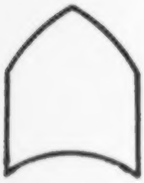
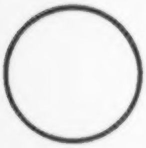
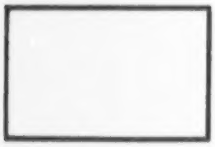
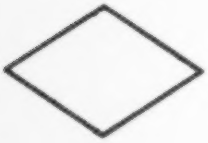
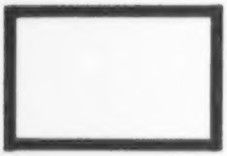
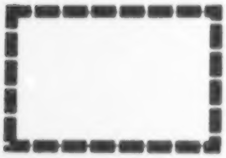
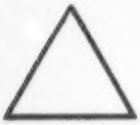


EXHIBIT 4.11

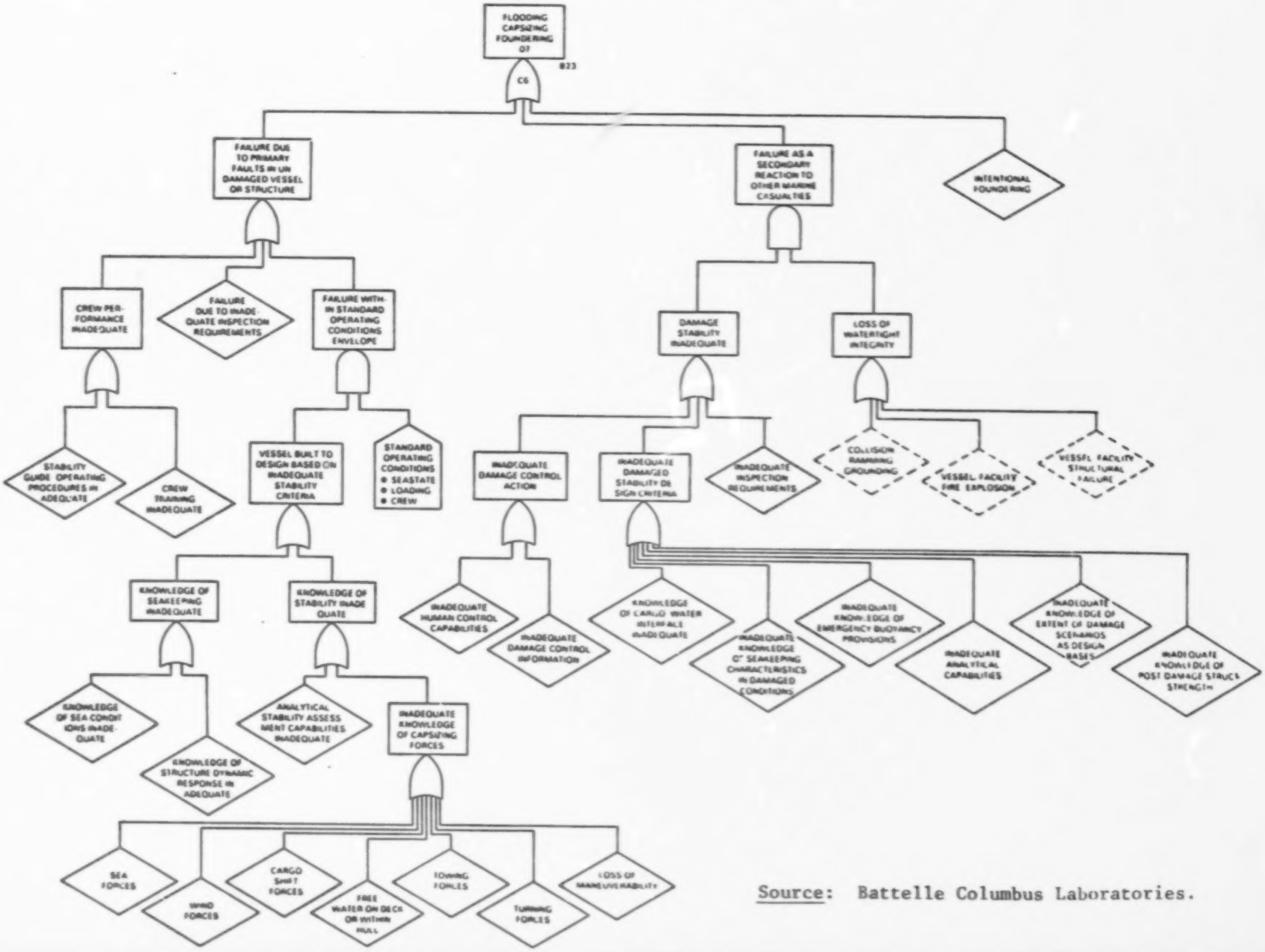
SYMBOLS USED IN LOGIC DIAGRAMS

	"AND" GATE	(Both lower events are required simultaneously to produce the upper event)
	"OR" GATE	(Any one of the lower events will produce the upper event)
	VOLUNTARY HUMAN INVOLVEMENT	
	STANDARD EVENT	(Developed further)
	STANDARD EVENT	(Not developed further)
	PRIMARY PROBLEM AREA EVENT	
	REPEATED PRIMARY PROBLEM AREA	
	TRANSFER SYMBOL	

LTA = LESS THAN ADEQUATE

EXHIBIT 4.12

LOGIC DIAGRAM FOR PRIMARY PROBLEM AREA 07, FLOODING, CAPSIZING, FOUNDERING


FLOODING CAPSIZING FOUNDERING 07
823
C6
FAILURE DUE TO PRIMARY FAULTS IN UN DAMAGED VESSEL OR STRUCTURE
FAILURE AS A SECONDARY REACTION TO OTHER MARINE CASUALTIES
INTENTIONAL FOUNDERING
CREW PER-FORMANCE INADEQUATE
FAILURE DUE TO INADE-QUATE INSPECTION REQUIREMENTS
FAILURE WITH-IN STANDARD OPERATING CONDITIONS ENVELOPE
DAMAGE STABILITY INADEQUATE
LOSS OF WATERTIGHT INTEGRITY
STABILITY GUIDE OPERATING PROCEDURES IN ADEQUATE
CREW TRAINING INADEQUATE
VESSEL BUILT TO DESIGN BASED ON INADEQUATE STABILITY CRITERIA
STANDARD OPERATING CONDITIONS
● SEASTATE
● LOADING
● CREW
INADEQUATE DAMAGE CONTROL ACTION
INADEQUATE DAMAGED STABILITY DE SIGN CRITERIA
INADEQUATE INSPECTION REQUIREMENTS
COLLISION RAMMING GROUNDING
VESSEL FACILITY FIRE EXPLOSION
VESSEL FACILITY STRUCTURAL FAILURE
KNOWLEDGE OF SEAKEEPING INADEQUATE
KNOWLEDGE OF STABILITY INADE QUATE
INADEQUATE HUMAN CONTROL CAPABILITIES
INADEQUATE DAMAGE CONTROL INFORMATION
KNOWLEDGE OF CARGO WATER INTERFACE INADEQUATE
INADEQUATE KNOWLEDGE OF SEAKEEPING CHARACTERISTICS IN DAMAGED CONDITIONS
INADEQUATE KNOWLEDGE OF EMERGENCY BUOYANCY PROVISIONS
INADEQUATE ANALYTICAL CAPABILITIES
INADEQUATE KNOWLEDGE OF EXTENT OF DAMAGE SCENARIOS AS DESIGN BASES
INADEQUATE KNOWLEDGE OF POST DAMAGE STRUCT STRENGTH
KNOWLEDGE OF SEA CONDIT IONS INADE-QUATE
KNOWLEDGE OF STRUCTURE DYNAMIC RESPONSE IN ADEQUATE
ANALYTICAL STABILITY ASSESS MENT CAPABILITIES INADEQUATE
INADEQUATE KNOWLEDGE OF CAPSIZING FORCES
SEA FORCES
WIND FORCES
CARGO SHIFT FORCES
FREE WATER ON DECK OR WITHIN HULL
TOWING FORCES
TURNING FORCES
LOSS OF MANEUVERABILITY

Source: Battelle Columbus Laboratories.

The Primary Problem Area (PPA) Logic Diagram developed to form the basis for the eventual Coast Guard Safety plan is shown in Exhibit 4.10. This exhibit contains a few basic symbols which are defined in Exhibit 4.11. The key symbol here is the Primary Problem Area box, which is thickly outlined, in contrast to the thinner outline of the standard event. The aim of the Primary Problem Area Logic Diagram is, through the use of fault-free analysis techniques, to trace undesirable events at the top (parties-at-risk) to a set of basic faults (i.e., primary problem areas). The linkage of events is through AND and OR gates, as the case may be.

P.P.A. No. 1, "Problem Analysis, Definition and Management Information" is not shown in Exhibit 4.10 since it is the problem common to all levels of hazard analysis and hazard control activity. In this respect, it is not only a basic problem of the U.S. Coast Guard, but will inevitably remain a major focus of TDC interest in the area of transportation safety R&D.

For purposes of defining and developing individual RDT&E Projects and Tasks, it was necessary to continue the problem dissection process one step further to the sub-problem level. Each of the 14 Primary Problem Areas was further partitioned in this manner. Exhibit 4.12 is shown to illustrate the result of this problem disaggregation process with respect to PPA No. 7, Flooding, Capsizing and Foundering.

The following sub-sections will briefly describe the approach followed by the study team in carrying out each of the planning tasks faced by the authors of the Plan document.

4.8.2 Identification of Marine Safety Problem Areas

The establishment and subsequent mapping of RDT&E needs by means of the logic diagrams described above was accomplished on the basis of "top down" analysis of problem logic on the one hand, and also a "bottom up" process of problem identification achieved as a result of workshop sessions with Coast Guard staff, examination of project rationales already developed, creative suggestions from third parties and other sources. The process is therefore both deductive and inductive. Logically, the process starts by identifying or postulating some top-level undesired event such as the "occurrence of a marine casualty" which must then be analysed (i.e., broken down) into the various individual causes of error or system failure (hazard/problem elements or areas). The AND/OR gates of the diagram are used to distinguish between causes which must operate simultaneously for an event to occur (AND events) and those which can operate independently (OR events or causes).

Practically however, the "logic" must be established inductively from whatever source of information is available. The principal difference between the UMTA/OSPQ and Coast Guard studies in this repect is that the UMTA/OSPQ study made an attempt to quantify hazards (though not hazard probabilities) by means of a statistical analysis. The Coast Guard did not attempt to provide a formal statistical analysis of accidents. It merely proceeded by partitioning the general marine casualty problem into six sub-events, each of which denotes a set of events creating hazard for a particular element of the marine domain. The relative weighting of these hazards (problem areas) was not quantified or qualified in any way. However, the actual designation and delimitation of problem and sub-problem areas implies a claim to significance, though a significance based on informed judgement and deductive logic only.

4.8.3 Identification of Marine Safety RDT&E Project Areas, Projects and Tasks

A RDT&E marine safety Project Area is developed in the form of a coherent, individually organized set of activities aimed at solving the RDT&E - susceptible part of a Primary Problem Area. Project and problem areas are synonymous except that the latter is the result of looking at the accident event (and its causes) from the point of view of problem definition, whereas the former is directed to problem solution. Project Area titles thus suggest the kind of activities required (e.g. prevention, containment, minimization, etc.) to reduce or control hazards and mitigate the consequences of events described in terms of the Primary Problem Areas. Project Areas are too gross for RDT&E planning purposes, and the Plan itself is therefore developed in terms of a three-level structure of Project Areas, Projects and Tasks.

The individual RDT&E Projects making up a Project Area were designed to address the individual sub-problems revealed in the problem dissection process. The output of a project is thus a solution to an RDT&E - susceptible problem in marine safety. No projects are designed specifically as inputs to other projects except the analytic work proposed as a solution to Primary Problem Area No. 1, Problem Analysis and Management.

The Tasks related to the various RDT&E Projects are the individual work elements of the Project, the sequence of steps necessary in doing the project. They are described in the form of commands such as "conduct a systems analysis", "study and critique the state-of-the-art" or "develop an analytical model". These tasks are activities that can all be separately evaluated and accounted for. However, they contribute to the realization of marine safety goals only when their results are integrated with those of the other tasks in a particular project; they do not individually solve or mitigate any of the defined problems.

Development of project and task descriptions was a collective effort on the part of the study team. Discussion and workshop meetings were conducted to develop a consensus regarding the basic structure and content of the RDT&E Plan, based on the problem dissection and identification process. No specific "methodology" was followed. However, two projects were established in Project Area No.1 for the specific purpose of developing methodologies for making assessments of risk levels associated with marine transportation casualties and evaluating alternative methods of managing these risks. A project was also proposed with a view to designing a marine information system to provide the necessary management information for further analytic work, including forecasting of future developments related to marine safety.

4.8.4 Project Evaluation and Prioritization

The RDT&E Plan for marine safety was designed without constraint as to budget or externally imposed requirements for milestone accomplishments. The programming function, or the art of evaluating and selecting projects was not performed by the study team. However, the study proposed certain guidelines which are covered in this and the following sub-section of the present report.

Project evaluation implies the existence or establishment of standards or criteria by which the evaluation is undertaken. Three criteria were identified for this purpose as follows:

- Benefit or the degree to which an RDT&E item contributes to the solution of the RDT&E susceptible part of the marine safety problem;

- Benefit/cost or the effectiveness with which an RDT&E item utilizes budget committed to it;

- Project interdependency or the degree to which another item in the RDT&E Plan is dependent.

It is recognized that many other tangible and intangible criteria may be adopted by management decision-makers in the course of the evaluation process. Selection of these is not regarded as part of the planning function. However, assembly of information on the items proposed above is considered appropriate in providing a highly useful framework of "objective" priority factors with which effective decisions can be made.

A structured method of reviewing, evaluating and prioritizing projects on the basis of each of these three potential project evaluation criteria is presented. Benefits are allocated to projects on the basis of the "seriousness" of the safety problem that the project is designed to address. The problem is simplified by recognizing that relative rather than absolute benefit measures are all that are required to order the relative priorities of RDT&E projects. The allocation process is in two stages as follows:

- evaluate/measure the relative "seriousness" of marine safety problems;

- weight these measures according to the degree to which a given RDT&E item is thought to contribute to the solution of the problem.

The "seriousness" of the marine safety problem is the perceived seriousness of the problem from the point of view of the Coast Guard M/W offices. "Seriousness" is defined or rather thought of as the perceived risk involved in allowing that problem to go unresolved, risk being equivalent to the expected loss associated with the problem. For example, if accidents are implied, then the expected loss would be the product of the estimated losses per accident and the frequency of occurrence. If the problem is failure to develop improved procedures, then the expected loss would be the savings the improvement might have achieved. Losses may include tangible loss (dollars) as well as intangibles such as human suffering, loss of well-being, negative image for the Coast Guard etc.

Problem evaluation is conducting with the assistance of the problem logic diagrams. An arbitrary numerical value of 100 is assigned to the "total" marine domain casualty problem (event A). This is then progressively sub-divided and allocated to the parties-at-risk, the primary problem and sub-problem areas through a judgemental assessment of the seriousness factor. At the level of individual parties-at-risk, the rationale used was as follows:

- The average value for each event, if each were judged equally serious would have been 16-2/3.

- The risk involved with cargo losses should be less than the average since protection of cargo has not been given major emphasis as a Coast Guard responsibility in the same way that protecting the marine environment has, for example. Further, by definition, human life or well-being is not involved with this party-at-risk.

- Vessel and facilities risk involve substantial loss potential from accidents and there is more pressure on the Coast Guard to protect these parties-at-risk.

- The other parties-at-risk involve hazards to people or the marine environment which involve the largest risks overall.

Once these value are assigned, they are then further apportioned among the primary problem and subproblem areas down through the trees. At each junction, the evaluation was made subjectively with some reference to statistics on marine casualties, cost of accidents and the like. However, no definitive "method" was employed throughout. Quantitative analysis was always leavened with study team impressions of a variety of intangibles concerning trends in marine casualties and in the emergence of hazards associated with technological change and so forth.

The values accumulated for each primary problem area are termed "P_t's".

Step number two was the procedure used to allocate benefit values to project areas and projects. This was done on the basis of a two-fold weighting scheme which embodied:

- an "access" factor (f_a);
- an "effectiveness" factor (f_e).

The access factor is the fraction of the primary problem that the RDT&E project could solve if it were successful i.e. the RDT&E susceptibility factor. The effectiveness factor is an estimate of the likelihood that the project will be successful in meeting its avowed objectives. RDT&E project benefit or Nb may thus be described mathematically as:

$$N_b = P_t \times f_a \times f_e$$

Judgemental evaluation of all projects on this basis can lead to a first "strawman" prioritization for RDT&E projects. This result may then be used as a baseline for a continuous process of re-evaluation and assessment by program management.

The benefit-cost criterion (N_{b-c}) may be established by dividing the N_b figure for a given project by a project-related cost expressed in $ millions. Costs of the project life (including implementation cost) should be expressed in terms of present values. In this manner, "benefit units" may be expressed as units per $ million of R&D funds.

The project interdependency criterion is important to the extent that projects exhibit a significant amount of "cross-talk" or exchange of data, information and mutual reinforcement of benefit, in pursuit of their independent objectives. This factor provides an important means of reducing duplication of effort and of promoting plan efficiency. Unfortunately, it also significantly complicates the process of project evaluation.

The study developed a project interdependency display diagram which made it possible to recognize at a glance, the existence and direction (though not the degree) of project interdependency. A project generally supports another or others by providing inputs of data, methods or technology. These inputs may be vital, helpful or merely of a coordinative nature such as common standards, methods or techniques with respect to some operation such as manpower training or materials inspection.

These support activities, mutual dependencies or mutual reinforcement activities must be evaluated in terms of how they affect access and effectiveness values.

4.8.5 Project Selection and Budgeting

A distinction must be made between project selection criteria and project evaluation criteria. If ten projects are selected, they would not normally consist of the top ten on the priority list. Criteria for project selection must be a function of the prevailing budgetary, technological and political environment of the Coast Guard and cannot be established by scientific method. However, certain guidelines may be given.

Budgetary criteria may include the truncation of projects on the basis of priority measures, but could also include other criteria such as:

- maximize program benefits;

- perform some work on all projects (either by stretching the time frame for implementation or by reducing the scope of work);

- establish budget limits on a Divisional basis;

- establish budget limits by Primary Problem Area.

Technological criteria relate to changes in the environment that may reduce the need for conducting RDT&E activity in a given area. For example, economic changes could lesson the need for the establishment of deep water offshore ports or a particular project might encounter insuperable technical difficulties.

Political criteria relate to public pressures for increased attention (and funding) in certain areas, particularly in the wake of catastrophic accidents. In theory at least, on-going work in PPA No.1 would reduce the incidence of this factor by identifying and correcting potential trouble-spots in advance. This would be achieved on the basis of an ongoing RDT&E plan update process.

5. AN APPROACH TO IDENTIFYING SAFETY R&D NEEDS

5.1 Introduction

Review of the state-of-the-art reveals that results of attempts to come to grips with the problems of transportation safety program and R&D project planning have been mixed. Two facts are apparent:

- The development and application of systematic approaches/methods to assist in establishing safety need areas has received low priority in transportation agencies, partly as a result of a lack of institutional focus for the transportation safety mission, partly due to the relatively low mission-dependency on R&D.

- The principal barrier to a "system safety" approach to transportation safety R&D needs establishment is the paucity of suitable data.

The data problem is clearly apparent in both the UMTA/OSPQ and Coast Guard studies, both of which attempted to apply a "system safety" approach to the establishment of transit and marine needs respectively. It is a problem which is, if anything, more acute in Canada, partly as a result of the high cost of the data, partly as a result of the complexity of transportation systems and the fragmentation of jurisdictional responsibility for and control of the various transportation modes.

In view of this situation, the most appropriate approach would appear to be the building block approach taken by the Coast Guard study. At this stage, only the basic framework for the approach can be given. However, the building blocks themselves may be identified and assembled on a step-by-step basis as more detailed data and more powerful tools are developed. No purpose would be served by attempting to take the gates of heaven by storm before developing the means of getting off the ground.

This basic philosophy of the Coast Guard study has been used as the model for the approach developed in the text that follows. It is presented in two parts. First is a summary description which emphasizes flexibility with respect to problems of data. It makes the best use of available data and makes provision for the identification and development of improved data quality. In other words, the implicit premise is that R&D planning must still take place, even without ideal data. Any planning method must be able to work in the initial instances with available data.

Second, we apply the method to the air mode. This application is in the nature of a demonstration. Logic diagrams are constructed to identify, on a first-cut basis, the primary problem areas and ways are discussed to estimate the "seriousness" of each problem area. However, the development of the corresponding R&D project areas, and projects, is beyond the scope of this study. It would require expertise from CATA to provide the appropriate inputs for this.

A number of conclusions that emerge from this initial demonstration and application to the air mode are discussed in a final section.

5.2 Framework for an Approach to Identifying Transportation Safety R&D Needs

The development of a safety R&D plan, based on the approach proposed in this report, is a three-step process:

1. development, through a logical fault-free analysis, of an understanding of the primary (safety) problem areas and of subproblems which are at least partly susceptible to R&D solutions;

2. development, with the expertise of safety and modal experts, of an inventory of R&D project areas and specific R&D projects which are capable of addressing the R&D susceptible portions of the problem areas;

3. programming of R&D projects. This requires evaluation, ranking and selection of individual projects, based on measures of project benefit as contributing to the solution of individual safety problems.

It is Steps 1 and 2 that constitute the identification of the totality of safety R&D needs. Step 3 brings in relative benefit and budget considerations for the selection of packages of R&D projects for programming purposes. The focus of this report is on the first two steps, although their linkage to step 3 is discussed as well (particularly, Section 5.2 following).

The above approach is inspired very largely from the U.S. Coast Guard methodology described in Section 4.8 and some repetition is therefore inevitable. In addition, we also summarize the tasks involved in the programming step 3 (above) which immediately follows the establishment of safety R&D needs.

The following are the major tasks which are described more fully in subsequent subsections:

- establishment of safety R&D core team;
- definition of the role of R&D in support of agency safety mission;
- development of problem dissection procedures;
- identification of primary problem areas (PPA's);
- subproblem analysis;
- R&D project identification;
- R&D project evaluation;
- R&D project selection.

The first five tasks together constitute step 1. The sixth task is step 2 and the remaining two tasks together make up the programming phase (step 3). One of the more obvious primary problem areas will inevitably be the lack of suitable data and tools of analysis with which to carry out the above tasks. This is in itself a task which is described in the sub-section entitled "management information problem area".

The following will briefly describe each of these activities in turn.

5.2.1 Establishment of Safety R&D Core Team

The quality of project identification and selection will depend as much on the quality of the personnel involved in the study process as on the quality and quantity of the information available. The establishment of the core team is thus a key factor of success. However, the exact composition of such a group will depend on administrative and organizational practices within the relevant agency. In the case of the U.S. Coast Guard, this team was made up of representatives from the program offices and administrative elements at Headquarters. Meetings were arranged in the form of seminars on research support needs under the direction of Batelle Columbus Laboratories. However, a number of different formats and formulae may be envisaged, based on the needs/practices of the agency involved.

Ideally, this group should include both safety and modal technical people as well as representatives from management.

5.2.2 Definition of the the role of safety R&D

The first task of the above core group would be to develop a consensus with respect to the safety mission of the agency and of the role of R&D in the fulfillment of mission objectives. This could be undertaken in a formal committee or seminar setting. Past and on-going safety activities including R&D activities in support of the mission, should be reviewed and the role of R&D determined. This may be formalized in the form of a statement which outlines the relevant "domain" of the agency in the safety field and the support provided by R&D. For example, in enforcing laws regarding spills as part of its mission, the Coast Guard may need the technological capability to detect them and respond in an effective and timely manner. In this case, R&D may have an operational role in assisting the development of detection devices, procedures, etc.

In this mission context, the external "problem" is the potential occurence of accidents. The internal problem is the institutional barriers (lack of resources, mandate, knowledge) to solve the external problem. The role of R&D is to reduce the potential for accidents and mitigate their consequences. Only part of the external problem, however, is solvable by R&D. In the identification of R&D needs, therefore, the basic approach is to seek out the "R&D susceptible" portions, and develop R&D projects to solve them.

5.2.3 Development of Problem Dissection Procedures

The general safety "problem" may be described as the potential occurrence of accidents with any of the following results:

- injuries/fatalities;
- significant property damage;
- environmental damage.

The problem dissection process involves a top-down approach to identify successively more detailed dissections of the general problem to create a hierarchy of subproblems. It is useful to use logic (fault-tree) diagrams to represent the results of this process. These diagrams use the AND/OR logic symbols described in Section 4.8 to record the problem/subproblem array and to clarify the relationships between subordinate problem events. The logic diagrams have the following main levels in their hierarchy:

- top level: undesired event or general problem - the accident;
- second level: subdivision of the undesired problem event: usually a list of "parties-at-risk" which may be injured or damaged in the potential accident;
- lower (subproblem) levels: represent faults in the transportation system or causes of the damage or injuries in the second level breakdown noted above. Thus, lower levels represent possible causes/faults or precursors of the events in the higher levels.

The problem dissection process should be carried out with detailed inputs from the study group. The output is a systems description of the particular transportation system in terms of a logical structure of faults (fault-tree) which can result in the undesired event, an accident. It should be noted that the top two levels are not "faults" in the strict engineering sense often associated with fault-trees. They are, however, undesired events. The rest of the subproblems represent, in fact, faults or failures in the system.

The degree of subproblem dissection is a function of the ability to relate mission activities to them and to define the internal problems present that might be solved or mitigated through R&D action. In this light, the following primary problem concept is important.

5.2.4 Identification of Primary Problem Areas (PPA's)

This is one of the most significant steps in the identification of R&D needs. The term "primary problem area" designates a unique, generic type of system failure or accident having two characteristics:

- it can potentially result in an accident;
- it involves a single sector of technology within which a coherent set of hazard control actions can be organized.

In most cases, primary problem areas act as first or basic causes of the parties-at-risk events. Primary problem areas provide the basic organizational structure for identification of R&D needs and subsequent R&D planning and management.

5.2.5 Subproblem Analysis

Each of the primary problem areas is further analyzed in fault-tree diagram form to the level of detail at which R&D susceptible sub-problems become clarified or evident to the study group.

The final extent of this process is a function of the study group's experience, abilities and judgement. That is, at the lowest level of problem dissection, the identified subproblems should clearly be susceptible to specific, project-describable R&D responses.

5.2 6 R&D Project Identification

In essence, the process of systematically dissecting the top level safety problem terminates when R&D susceptible subproblems are identified by the study group. The translation of these needs into a comprehensive set (or "wish list") of R&D projects involves a complementary series of project descriptions as follows:

- "Project Area" refers to the potential set of R&D efforts which may be directed to a particular primary problem area;

- "Projects" are individual activities within a project area designed to addresss individual subproblems (or primary problem areas) revealed in the problem dissection process.

- "Tasks" refer to the sequence of related steps necessary to complete a project.

The problem dissection process, therefore, results in a complete (exhaustive) list of R&D projects (as judged by the study team) to solve the current safety problem.

5.2.7 R&D Project Evaluation

Agency budget constraints generally make it difficult, if not impossible, to undertake all the various R&D projects identified. The tasks involved in determining how agency resources are applied towards the achievements of mission objectives in the field of transportation safety make up the programming phase of safety R&D planning. These tasks are essentially threefold:

- evaluate projects in terms of their relative contribution to solving the problem and the costs of carrying them out;

- rank and select the most cost-effective projects;

- fund projects for a particular fiscal period (not covered below).

The first of these tasks, the evaluation of individual projects, is based on the potential contribution that may be made by the project towards the achievement of agency mission objectives. This contribution is evaluated in terms of:

- the "benefit value" P_t of solving a problem measured in terms of problem "seriousness" or the expected losses involved in allowing the problem to go unresolved;

- the "access factor" f_a or degree to which the particular problem is susceptible to solution by means of the R&D project under review;

- the "effectiveness factor" f_e or probability of success of the project in question.

Problem seriousness may be measured in terms of the social, psychological and economic losses (lost human work efforts, etc.) attributable to accidents and their aftermath (fatalities, injuries and property damage). Losses of accidents which have occurred are often estimated with "accident costing models" which measure all losses in each accident in monetary terms. Thus, the distribution of such costs over the parties-at-risk would indicate the relative historical seriousness of each. The fault tree analysis would assist in distributing the value of losses over the primary problem areas.

However, the Coast Guard study initially adopted a more judgemental approach by distributing 100% of the safety problem over the primary problem areas (using the fault trees and any supplementary causal data linking problem area occurence probabilistically to the top level parties-at-risk).

This aspect of the methodology is thus closely linked to the problem dissection process, but is, in fact, carried out subsequent to the identification of the full set of projects.

5.2.8 R&D Project Selection

The final ranking and selection of projects is undertaken by ascribing an overall benefit value N_b to projects on the basis of the following:

$$N_b = P_t \times f_a \times f_e$$

A benefit/cost ratio N_{b-c} is then calculated by dividing the N_b value of the project with the anticipated costs of the project. The present value of project costs should be used when the cost stream is spread over several years.

The quantity N_{b-c} is thus a measure of the effectiveness of funding required to implement the project.

5.2.9 Management Information Problem Area

While the above framework has been proposed as an overall conceptual approach to the problem of developing methods to assist in establishing R&D needs in the field of transportation safety, the general absence of essential information and the lack of suitable tooks of analysis, will be an ever-present reality in most cases. This fact itself can thus become a primary problem area and perhaps the primary problem area. Each agency must determine for itself the scope of its own needs in this respect. In the case of the U.S. Coast Guard study, a number of "projects" were identified to fill gaps in this area. These include:

- forecasting of marine activity and technological change in the transportation environment;

- coordinating of the agency's information flows and sources;

- development of models and data with the ability to assess the risks and costs of accidents in order to evaluate relative problem seriousness.

In defining the terms of reference and other specifications for these various tasks, it is always important for the particular agency to remember that:

- the method is based on the mission of the agency;

- it requires a multi-disciplinary safety core team to bring a variety of perspectives to bear;

- it is based on safety problem dissection, using an analytical technique of system safety (fault-tree analysis);

- the processes of mission definition and problem dissection may be fairly time-consuming, and likely involve several iterations to arrive at a consensus result.

- the process is flexible and adaptable, in that it can make use of any and all data and expertise available;

- the higher the quality of the data which links problems (causes) to accident outcomes, the better will be the problem dissection process and the assessment of summary problem area seriousness.

The following sections of this chapter will further discuss this approach through the device of "demonstrating" its application to the air mode.

5.3 Approach to Identifying Safety R&D Needs in the Air Mode

5.3.1 Introduction

The following sub-sections make a first attempt to demonstrate the use of the Coast Guard technique for the air mode in Canada.

It should be emphasized that this is an initial attempt only , with many simplifications and assumptions. It is likely, even inevitable, that shifts in relative emphasis would occur if safety and other officials from CATA were involved in carrying out the process. Nevertheless, some insights into the use of the methodology can be gained. The primary problem area logic diagrams, and the subproblem breakdown of the primary areas differ in some significant ways from the Coast Guard approach, due to the quite different characteristics of the air mode in comparison to the marine mode.

We also describe ways in which the severity of the problem areas can be determined, using the "Costs of Aircraft Accidents" model previously developed for the Aviation Safety Bureau.

5.3.2 Main Elements of the Approach to Identify Safety R&D Needs in the Air Mode

5.3.2.1 CATA Safety Mission and "Air Domain"

The CATA Safety Mission is:

"to ensure that an adequate level of safety is provided for the national air transportation system".

From CATA activities and responsibilities, we infer that the Air Domain includes:

- aircraft, personnel, facilities (terminals, runways, communication and information systems), passengers, airspace and all private and commercial aviation activity of concern to CATA.

5.3.2.2 Top Level (Undesired) Event: Air Accident

Most safety management efforts are directed at the prevention or mitigation of air accidents. For the purposes of the subsequent analysis, we define an air accident as:

"An occurrence involving injuries/fatalities or significant property damage, or damage to the environment".

This definition varies from the usual definition through the addition of reference to the environment. This is included for the sake of completeness and illustration, since the environment may be considered to be at risk from an air accident (spillage of toxic chemicals, etc.).

It might also be argued that incidents are also top level undesired events. They place various parties in the system at risk, at least momentarily and have many of the same characteristics as accidents, except for the injury/damage consequences. We have excluded these occurrences formally, however, in the absence of a reliable data base for incidents.

5.3.2.3 Parties-at-Risk in an Accident

On the basis of injury to persons, or damage to property or the environment, the following is a list of the parties-at-risk in an air accident:

- crew;
- aircraft;
- cargo;
- facilities/infrastructure (e.g., runways, terminals);
- the public;
- the environment.

The totality of losses due to aircraft accidents is covered by the above six parties-at-risk. Exhibit 5.1 shows the logic diagram for the parties-at-risk. Some comments are in order regarding the above listing.

- we have included cargo as a party-at-risk, although protection of cargo may not play a major role in CATA's mission.

- as noted above, environment is included as a party-at-risk, even though the usual definition of air accident does not include aspects of environmental degradation.

- facilities/infrastructure are included, although these are seldom damaged in an aircraft accident.

As will be shown below, the major losses are in fatalities/injuries, and hull damage.

5.3.2.4 Seriousness of Safety Problem

The seriousness of the safety problems associated with each party-at-risk is sometimes estimated on the basis of the economic losses associated with each. One approach is to use the Aircraft Accident Costing Model developed for the TDC (Report TP 3496). On the basis of average of monetary losses in accidents for the years 1976-1979, a distribution (totalling 100%) was calculated, assigning a proportion of the total loss to each party-at-risk. (Crew/passenger losses are based on the economic value of lost work effort; environmental losses cannot reliably be estimated since they are not included in the current accident data base.)

The resulting distribution of losses (totalling 100%) is also shown in Exhibit 5.1. It can be seen that human losses are almost 2/3 of total losses and aircraft hull losses a little less than 1/3. All other parties-at-risk losses, when combined, account for only a small amount of loss.

5.3.2.5 Development of Primary Problem Areas

Using fault-tree techniques as the major tool for problem dissection, logic diagrams were developed for each of the parties-at-risk except cargo (which was judged to play a limited role at this time). These are shown in Exhibits 5.2 to 5.6.

Knowledge of the aviation system was subsequently applied to dissect the parties-at-risk problems to the level of primary problem areas.

The resulting list of primary problem areas is as follows:

- collision/crash inflight;
- fire/explosion inflight;
- aircraft systems primary failure;
- crashworthiness of hull less than adequate;
- fireworthiness of aircarft less than adequate;
- interior structural design of aircraft less than adequate;

- survival equipment/procedures less than adequate;
- infrastructure/facilities systems primary failure
- operational degradation of the environment;
    - discharge detection/response/control of harmful materials less adequate;
    - hazardous materials containment system primary failure.

Brief descriptions of the problem dissection process for the parties-at-risk are as follows:

- Aircraft-at-risk (Exhibit 5.2) - An OR gate leading to aircraft-at-risk indicates that any one of three primary problem areas can lead to damage of the aircraft: collision/crash, fire/explosion, aircraft systems primary failure (the use of the word "primary" indicates that this is the first failure occurrence. In contrast, aircraft systems may have a secondary failure in the event of a fire or explosion on board.).

- Crew/passengers-at-risk (Exhibit 5.3) - the first AND gate indicates that both an accident must occur, and on-board personnel are in jeopardy. An accident can occur through any one of the three primary problem areas as above. Personnel may be put in jeopardy as a direct accident casualty (which involves the three crashworthiness/fireworthiness/interior design primary problem areas), or as the result of inadequate survival procedures.

- Infrastructure/facilities-at-risk (Exhibit 5.4) - These are hazarded either through their primary failure, or through the effects of an accident, which again repeats the three basic causes of an aircraft accident.

- Environment-at-risk (Exhibit 5.5) - Environmental damage may result from regular operations (e.g., fuel exhausts) or from the presence of harmful material as the result of an accident. The latter requires that both discharge control is less than adequate and that the containment system is breached - the result of either the effects of an accident, or a primary failure in the material containment system.

- Public-at-risk (Exhibit 5.6) - The danger to the public is the result of combinations of the primary problem areas discussed above: the effects of an accident, operational environmental degradation, or presence of harmful materials (as above).

5.3.2.6 Identification of Subproblems susceptible to R&D solutions

The problem dissection process may be continued for each primary problem area to determine subproblems which are susceptible to R&D solutions. Again, using our understanding of the aviation system, we have analyzed selected primary problem areas to the subproblem level. The resulting fault-tree diagrams are shown in Exhibits 5.7 to 5.11.

Brief descriptions of the logic diagrams follow:

- Collision/Crash in flight (Exhibit 5.7) - This is likely the most complicated primary problem area. As depicted, all the fault events are related to either navigation system failures, or lack of aircraft navigation capabilities. In terms of navigation capabilities for example, there are three types of failure, related to:

  - human control capabilities;

  - lack of navigation information;

  - aircraft response capabilities.

The lowest level event boxes in the exhibit are all suggestive of subproblems that may be susceptible to R&D solutions. For example, "Navigation Aids Less than Adequate" suggests that R&D could identify and develop more effective navigational aids.

- Fire/Explosion in Flight (Exhibit 5.8) - Various failures leading to the top level event are indicated. Except for "Sabotage", the others may all be analyzed in the same way. A fire/explosion requires two failures: control is less than adequate, and failure of preventive measures. Failure of preventive measures always requires both: presence of flammable/combustible/explosive materials and an ignition source. Eliminating either one will prevent the fire/explosion. R&D may be applied, for example, to either one of these faults.

- Aircraft Systems Primary Failure (Exhibit 5.9) - The main causes of a primary failure are either inadequate design of systems or operational material degradation. In terms of design, it can be seen that there is wide scope for R&D in this area (e.g., basic research may be required in regard to materials structural performance). With respect to material operational degradation, the basic causes are improper maintenance or inadequate inspection procedures.

- Survival Equipment/Procedures Less than Adequate (Exhibit 5.10) - This is a fairly straightforward subproblem analysis, resulting in two main foci:

  - survival equipment/procedures adequacy;

  - personnel retrieval equipment/procedures adequacy; for example, adequacy of electronic locater transmitters (ELT).

- Operational Degradation of the Environment (Exhibit 5.11) - This type of environmental degradation occurs during normal aviation operations. Thus, it includes atmospheric and thermal pollution, noise and operations in fragile environments (e.g., some Arctic operations).

5.3.2.7 Aviation Safety R&D Needs and R&D Plan

The next logical step in the process is the development of Project Areas, Projects and Tasks to address the R&D susceptible portions of the subproblems identified above. (It is clear that the aviation safety study group would in reality be developing at least preliminary ideas in parallel with the problem dissection process.) The resulting exhaustive and unconstrained list of such projects would constitute the R&D needs for aviation safety.

It is beyond the scope of this study to suggest any specific projects to address the problem areas and subproblems identified on a preliminary basis in the preceding sections.

Similarly, it is also beyond the scope of this study to develop an R&D plan based on the resulting R&D needs. As described in Section 5.2.7, the development of an R&D Plan generally requires a method of evaluating individual projects to assess their benefit, or potential contribution to the safety problem. Rankings and selection may then be made. The benefit assessment methodology has been described in the case of the U.S. Coast Guard in Section 4.8.4.

5.3.3 Management Information Problem Area in the Air Mode

As already noted, this is an important ongoing research and development task, designed to facilitate and refine the analysis proposed in this report. As in the U.S. Coast Guard methodology, the application of this safety R&D needs identification approach in the air mode would also require some efforts in the following directions:

- provision of trend data for use in all R&D project areas:
    - major aviation technological trends;
    - traffic patterns;
    - siting of airport facilities;
    - cargoes to be carried;

- consideration of the coordination of all aviation safety related data bases (some work on this is currently ongoing in CATA);

- further development of risk models at the individual accident (micro) level, or geared to sub-components of the aviation system, to link causal factors or sequences to undesired outcomes, and attach probabilities.

- in conjunction with the risk models, further development if necessary, of costing models which can determine economic losses of accidents with specified characteristics. Such costing models also provide the capability of risk assessment at the aggregate or macro level for ongoing monitoring of the safety performance of the aviation system;

- both the above types of models, in their micro and macro applications, will assist CATA in providing measures of safety improvement resulting from R&D and other system changes.

5.4 Conclusions from the Demonstration of the Safety R&D Needs Identification Methodology in the Air Mode

Although we have conducted the preliminary problem-dissection analysis in the air mode without the benefit of a multi-disciplinary study group of aviation safety experts, we have, nevertheless, gained some insights into the application of the proposed R&D needs identification methodology:

- the methodology provides an organized, comprehensive systems approach to R&D needs identification;

- the analysis and development of logic diagrams for problem areas, and subproblems can be as detailed as resources, expertise, data and current understanding of the safety problem warrant;

- the methodology can therefore make the fullest use of available data and knowledge. But even if data and understanding of causal event linkages are less than ideal, the structure of the methodology remains unchanged - these lacunae are made up for by the expertise, experience and judgement of the multi-disciplinary core group.

- the methodology also incorporates, in parallel with current R&D plans, a further research project area to assist in rectifying data gaps and lack of understanding (this is the management information project area referred to in Section 5.3.3 above);

- the air accident data base (AIDS) is one of the most comprehensive modal accident data bases in Canada. It is therefore through analysis of causal factors, quite useful in assisting in the development of the logic diagrams by the problem dissection process.

In addition, an associated aircraft accident costing model has recently been developed which can estimate societal costs for individual accidents, and selected subsets of the total group of air accidents. This model is therefore extremely helpful in estimating the relative severity of problem and subproblem areas. For example, at the macro level, we were able to estimate the distribution of economic losses to the parties-at-risk in the aviation system (Section 5.3.2.4). Additionally, through the costing of appropriately selected subsets of accidents, the severity of primary problem areas may also be determined. Further analysis would be required to verify the extent to which this would assist in the problem-dissection process. These models can also be applied to estimate the improvements in safety due to R&D, and other system changes.

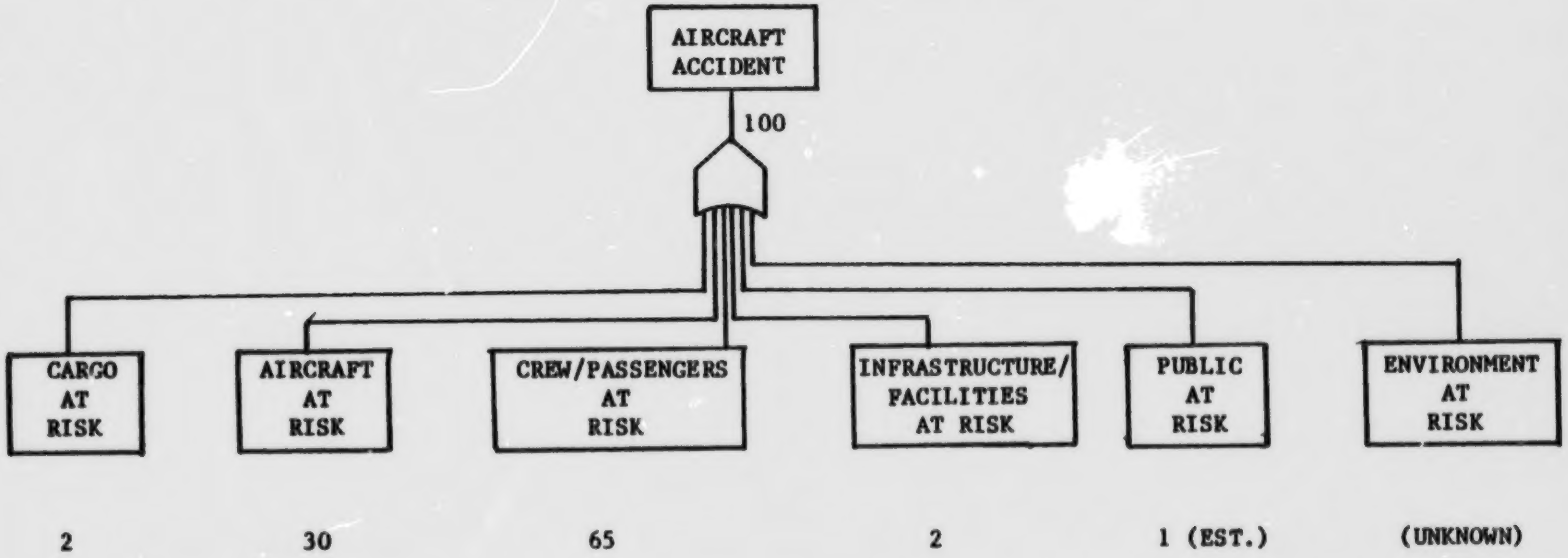
- some of the activities related to risk modelling and data coordination are already being assessed and developed in the National Air Transportation Safety Plan Study (NATSP), currently being undertaken by CATA. (A summary of the NATSP work plan is contained in Appendix A, Section A.4.2.4.) Some of the activities in NATSP include:

    - review existing safety information sources;

    - analyse safety management structure;

- develop event-tree descriptions of key infrastructure facilities;
- develop specific aviation system component models;
- provide overview of system risk.

It can be seen that these ongoing activities would be compatible with, and would provide many opportunities for enhanced data and understanding which could be used as inputs for the application of the proposed R&D needs identification methodology.


AIRCRAFT ACCIDENT
100
CARGO AT RISK
AIRCRAFT AT RISK
CREW/PASSENGERS AT RISK
INFRASTRUCTURE/ FACILITIES AT RISK
PUBLIC AT RISK
ENVIRONMENT AT RISK
2
30
65
2
1 (EST.)
(UNKNOWN)

NOTES 1. DISTRIBUTION OF LOSSES (i.e. safety problem seriousness) does not take into account the costs of SAR and other investigative/administrative costs (the Costs of Aircraft Accidents, TDC, TP 3496, December 1981).

2. Losses for crew/passengers are based on estimated lost value of productive work efforts (the Costs of Aircraft Accidents, TDC, TP 3496, December 1981).

EXHIBIT 5.1 LOGIC DIAGRAM SHOWING PARTIES AT RISK AND ESTIMATED SAFETY PROBLEM SERIOUSNESS (TOTAL=100)

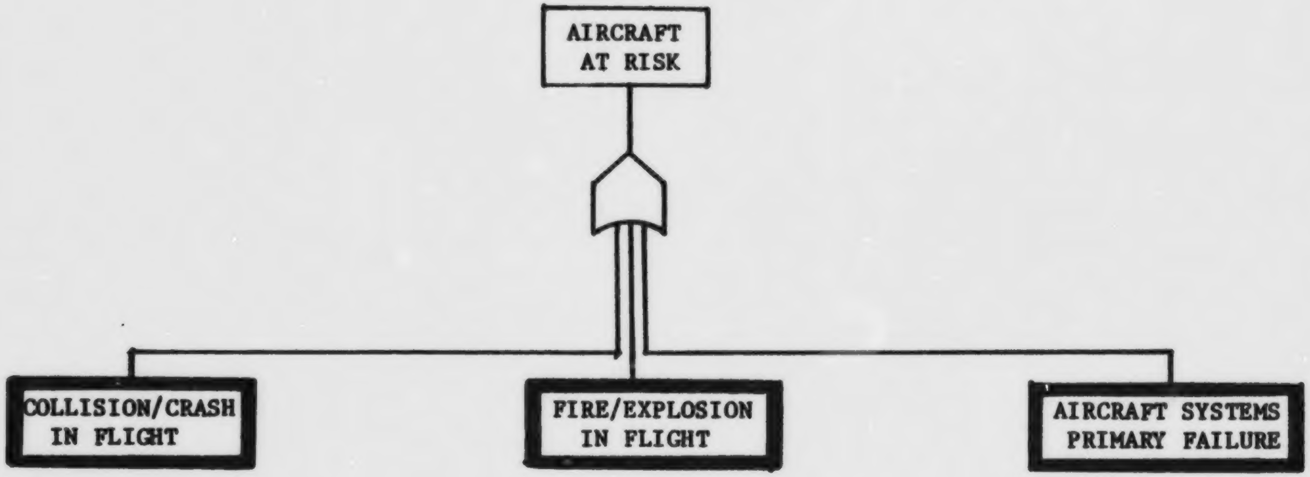

AIRCRAFT
AT RISK
COLLISION/CRASH
IN FLIGHT
FIRE/EXPLOSION
IN FLIGHT
AIRCRAFT SYSTEMS
PRIMARY FAILURE

EXHIBIT 5.2 LOGIC DIAGRAM SHOWING PRIMARY PROBLEM AREAS FOR "AIRCRAFT AT RISK"

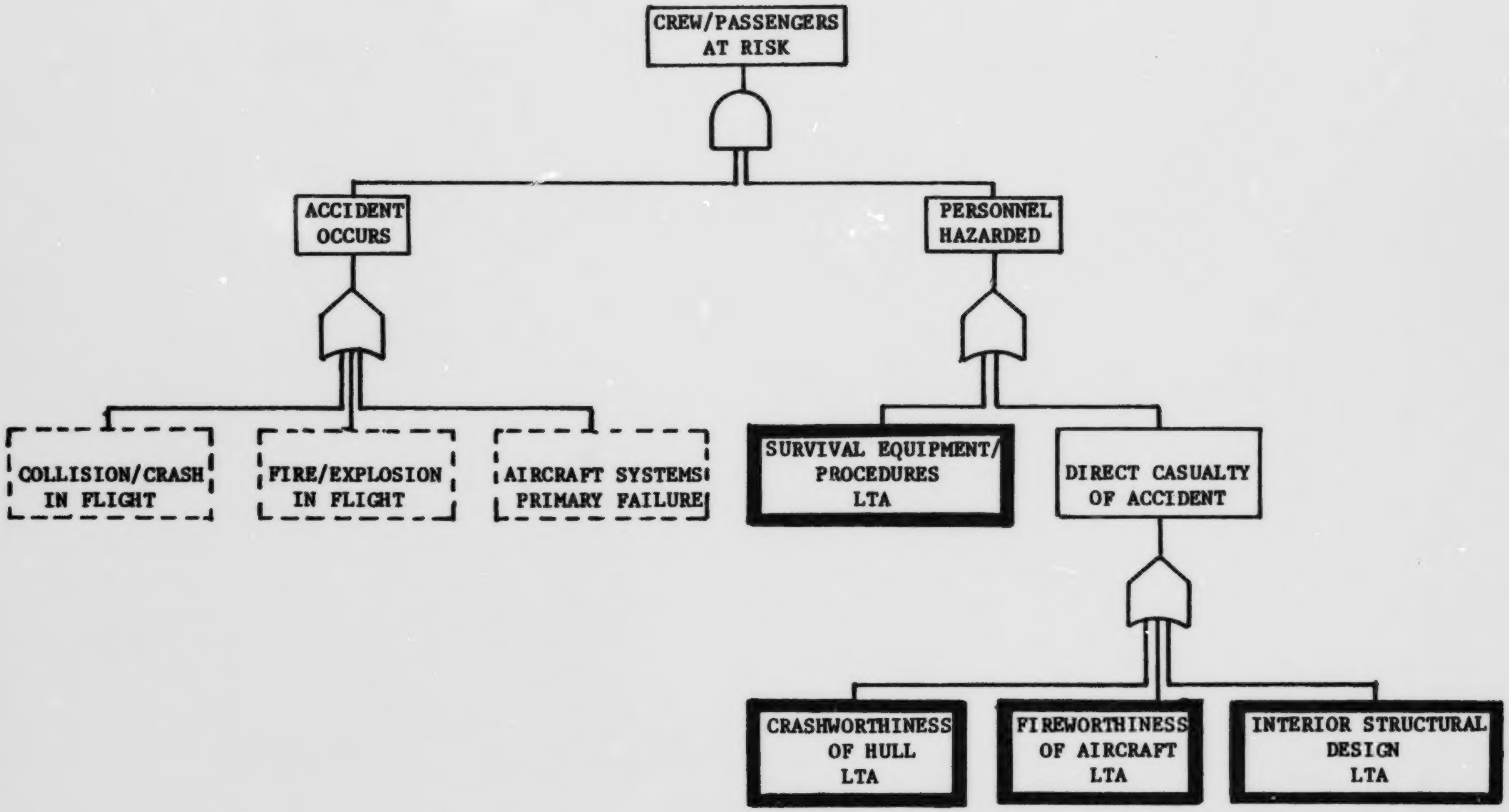

CREW/PASSENGERS AT RISK
ACCIDENT OCCURS
PERSONNEL HAZARDED
COLLISION/CRASH IN FLIGHT
FIRE/EXPLOSION IN FLIGHT
AIRCRAFT SYSTEMS PRIMARY FAILURE
SURVIVAL EQUIPMENT/ PROCEDURES LTA
DIRECT CASUALTY OF ACCIDENT
CRASHWORTHINESS OF HULL LTA
FIREWORTHINESS OF AIRCRAFT LTA
INTERIOR STRUCTURAL DESIGN LTA

EXHIBIT 5.3 LOGIC DIAGRAM SHOWING PRIMARY PROBLEM AREAS FOR "CREW/PASSENGERS AT RISK"

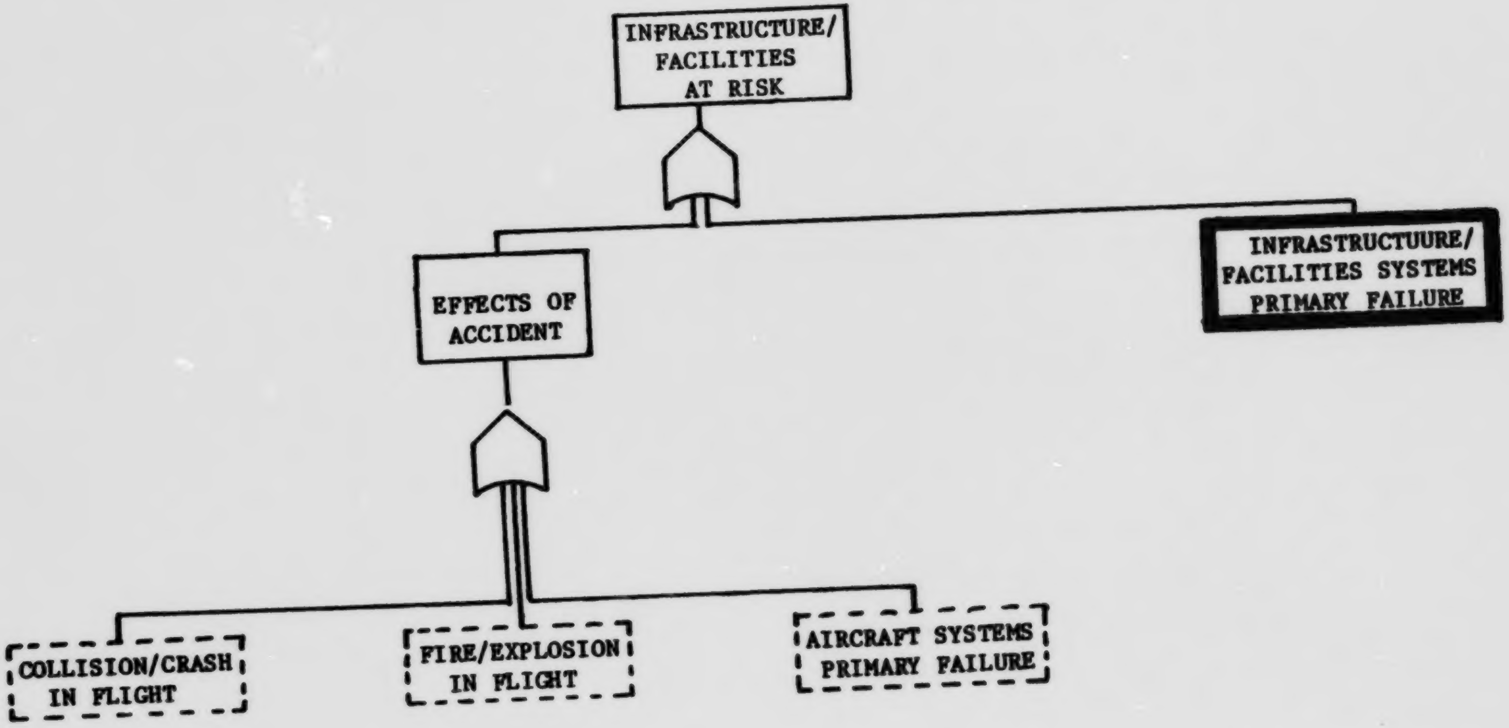

INFRASTRUCTURE/ FACILITIES AT RISK
EFFECTS OF ACCIDENT
INFRASTRUCTUURE/ FACILITIES SYSTEMS PRIMARY FAILURE
COLLISION/CRASH IN FLIGHT
FIRE/EXPLOSION IN FLIGHT
AIRCRAFT SYSTEMS PRIMARY FAILURE

EXHIBIT 5.4 LOGIC DIAGRAM SHOWING PRIMARY PROBLEM AREAS FOR "INFRASTRUCTURE/FACILITIES AT RISK"

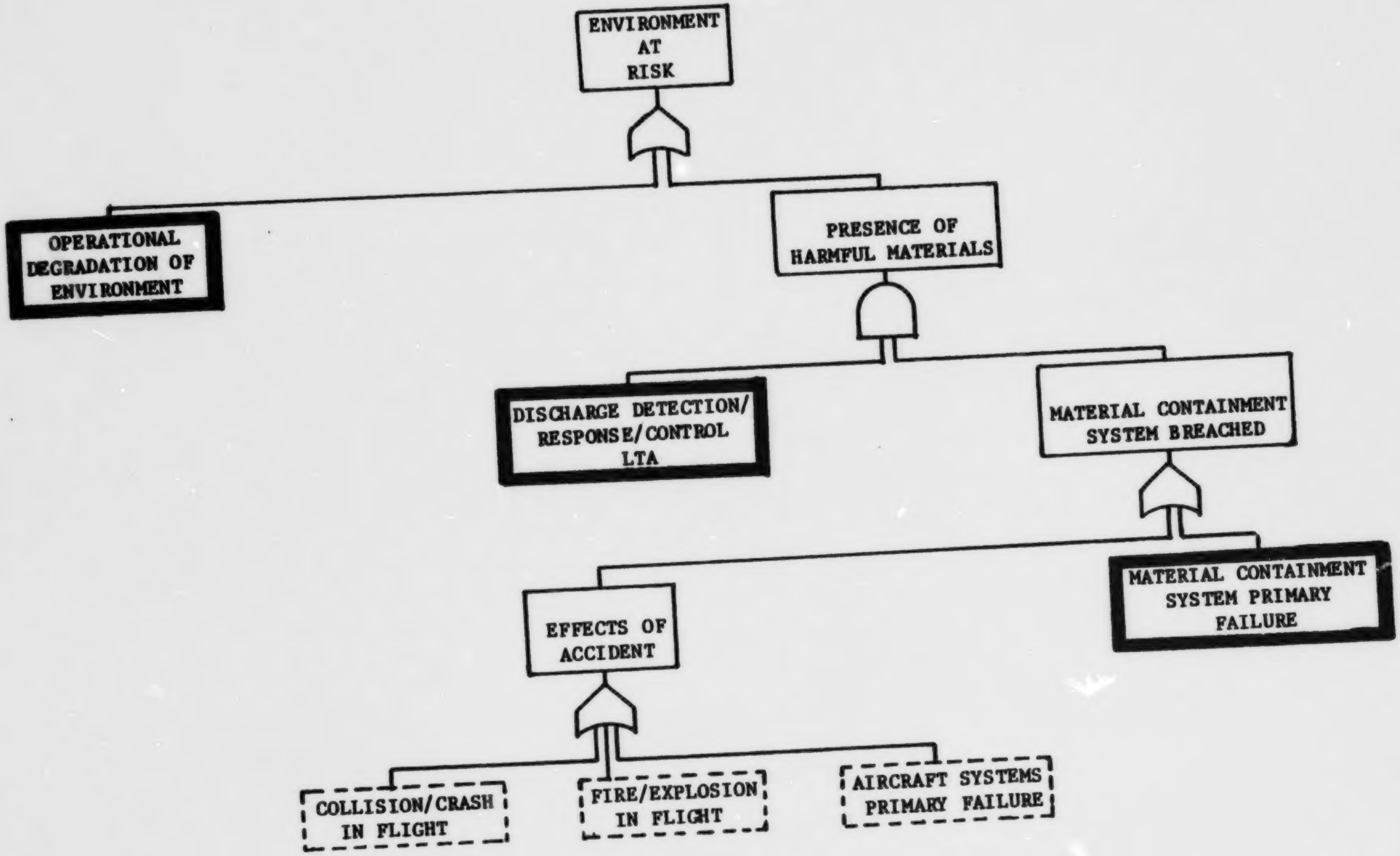

ENVIRONMENT AT RISK
OPERATIONAL DEGRADATION OF ENVIRONMENT
PRESENCE OF HARMFUL MATERIALS
DISCHARGE DETECTION/ RESPONSE/CONTROL LTA
MATERIAL CONTAINMENT SYSTEM BREACHED
EFFECTS OF ACCIDENT
MATERIAL CONTAINMENT SYSTEM PRIMARY FAILURE
COLLISION/CRASH IN FLIGHT
FIRE/EXPLOSION IN FLIGHT
AIRCRAFT SYSTEMS PRIMARY FAILURE

EXHIBIT 5.5 LOGIC DIAGRAM SHOWING PRIMARY PROBLEM AREAS FOR "ENVIRONMENT AT RISK"

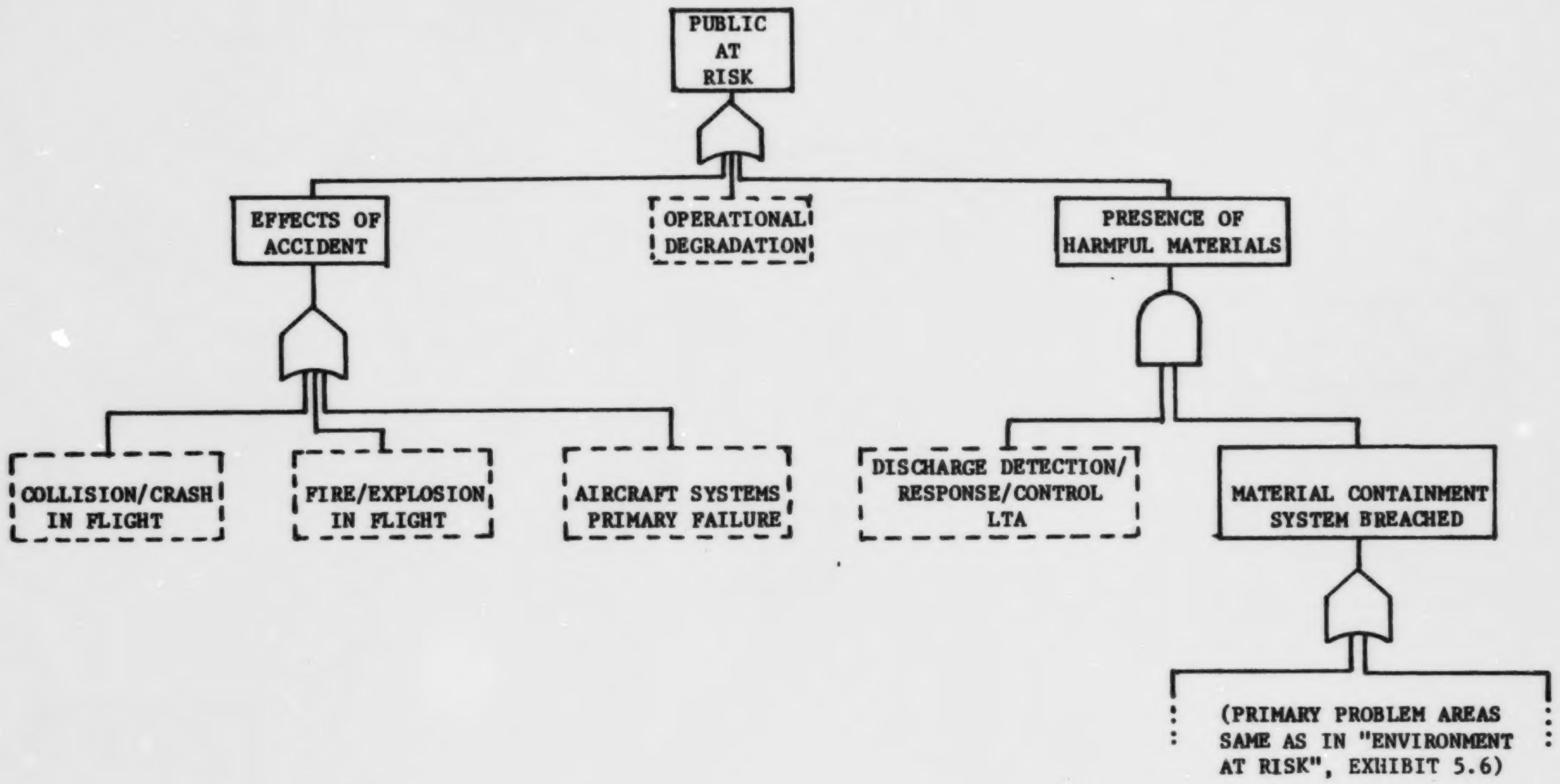

PUBLIC AT RISK
EFFECTS OF ACCIDENT
OPERATIONAL DEGRADATION
PRESENCE OF HARMFUL MATERIALS
COLLISION/CRASH IN FLIGHT
FIRE/EXPLOSION IN FLIGHT
AIRCRAFT SYSTEMS PRIMARY FAILURE
DISCHARGE DETECTION/ RESPONSE/CONTROL LTA
MATERIAL CONTAINMENT SYSTEM BREACHED
(PRIMARY PROBLEM AREAS SAME AS IN "ENVIRONMENT AT RISK", EXHIBIT 5.6)

EXHIBIT 5.6 LOGIC DIAGRAM SHOWING PRIMARY PROBLEM AREAS FOR "PUBLIC AT RISK"

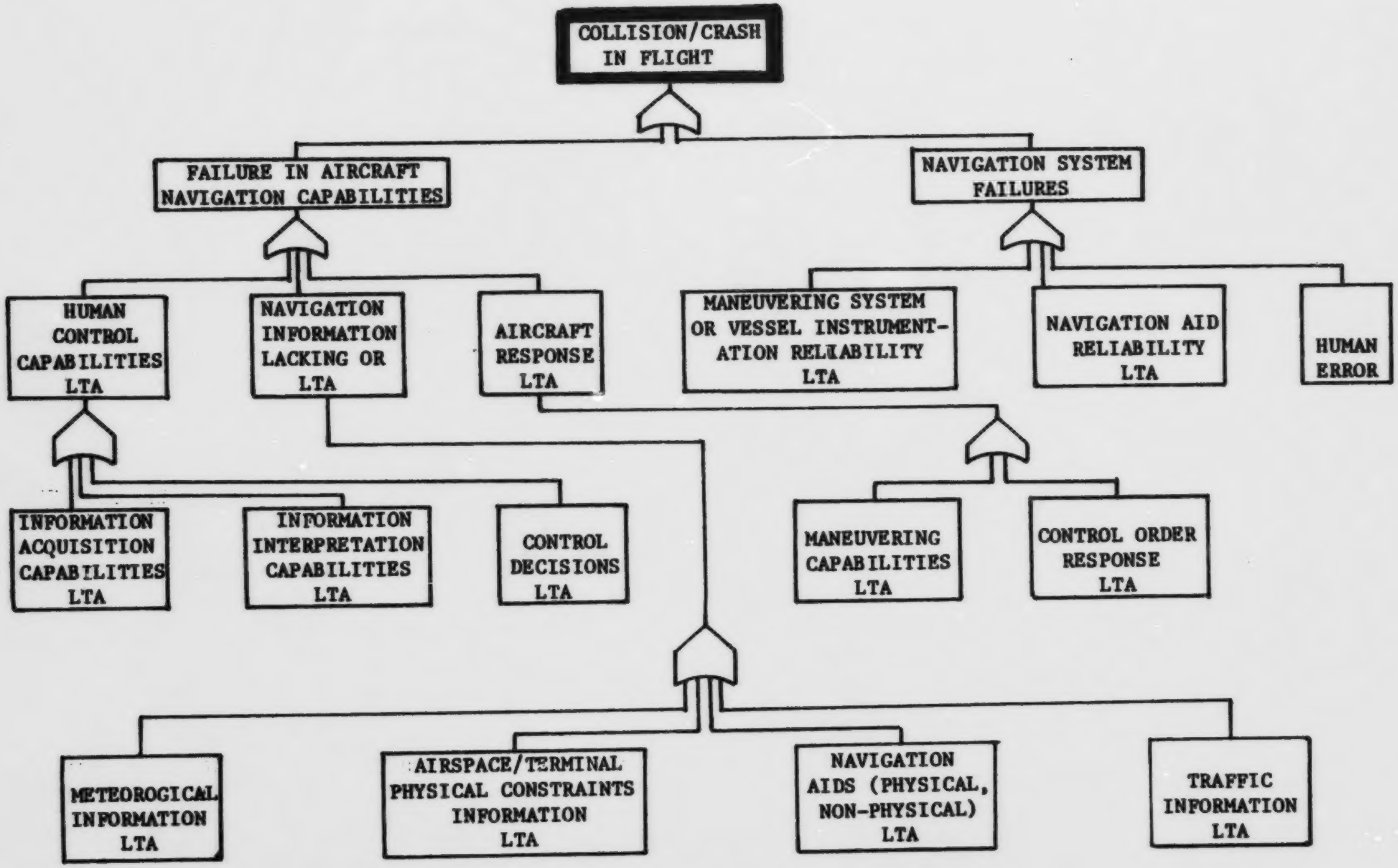

COLLISION/CRASH IN FLIGHT
FAILURE IN AIRCRAFT NAVIGATION CAPABILITIES
NAVIGATION SYSTEM FAILURES
HUMAN CONTROL CAPABILITIES LTA
NAVIGATION INFORMATION LACKING OR LTA
AIRCRAFT RESPONSE LTA
MANEUVERING SYSTEM OR VESSEL INSTRUMENTATION RELIABILITY LTA
NAVIGATION AID RELIABILITY LTA
HUMAN ERROR
INFORMATION ACQUISITION CAPABILITIES LTA
INFORMATION INTERPRETATION CAPABILITIES LTA
CONTROL DECISIONS LTA
MANEUVERING CAPABILITIES LTA
CONTROL ORDER RESPONSE LTA
METEOROGICAL INFORMATION LTA
AIRSPACE/TERMINAL PHYSICAL CONSTRAINTS INFORMATION LTA
NAVIGATION AIDS (PHYSICAL, NON-PHYSICAL) LTA
TRAFFIC INFORMATION LTA

EXHIBIT 5.7 SUBPROBLEM ANALYSIS FOR PRIMARY PROBLEM AREA "COLLISION/CRASH IN FLIGHT"

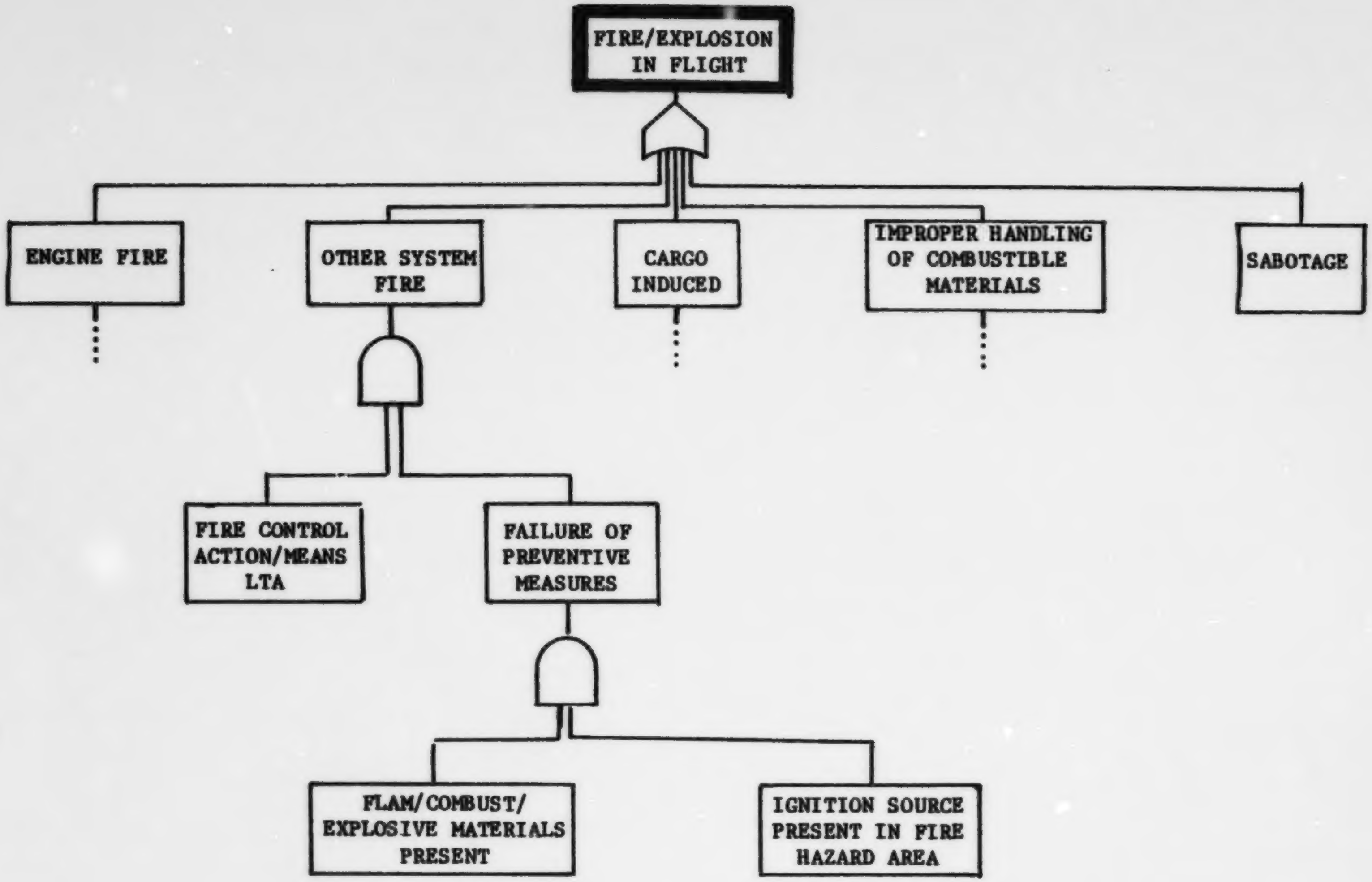

FIRE/EXPLOSION IN FLIGHT
ENGINE FIRE
OTHER SYSTEM FIRE
CARGO INDUCED
IMPROPER HANDLING OF COMBUSTIBLE MATERIALS
SABOTAGE
FIRE CONTROL ACTION/MEANS LTA
FAILURE OF PREVENTIVE MEASURES
FLAM/COMBUST/ EXPLOSIVE MATERIALS PRESENT
IGNITION SOURCE PRESENT IN FIRE HAZARD AREA

EXHIBIT 5.8 SUBPROBLEM ANALYSIS FOR PRIMARY PROBLEM AREA "FIRE/EXPLOSION IN FLIGHT"

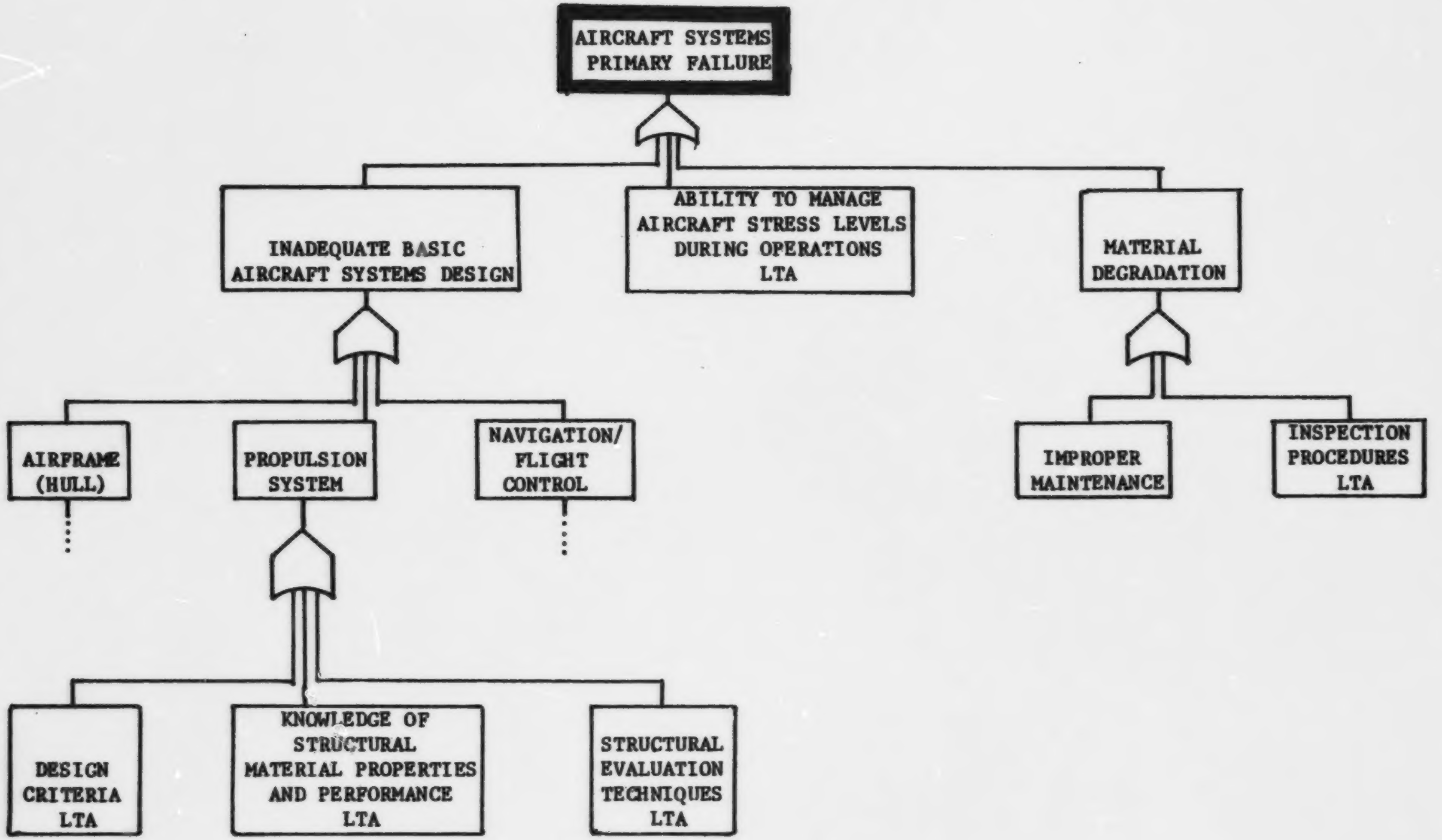

AIRCRAFT SYSTEMS PRIMARY FAILURE
INADEQUATE BASIC AIRCRAFT SYSTEMS DESIGN
ABILITY TO MANAGE AIRCRAFT STRESS LEVELS DURING OPERATIONS LTA
MATERIAL DEGRADATION
AIRFRAME (HULL)
PROPULSION SYSTEM
NAVIGATION/ FLIGHT CONTROL
IMPROPER MAINTENANCE
INSPECTION PROCEDURES LTA
DESIGN CRITERIA LTA
KNOWLEDGE OF STRUCTURAL MATERIAL PROPERTIES AND PERFORMANCE LTA
STRUCTURAL EVALUATION TECHNIQUES LTA

EXHIBIT 5.9 SUBPROBLEM ANALYSIS FOR PRIMARY PROBLEM AREA "AIRCRAFT SYSTEMS PRIMARY FAILURE"

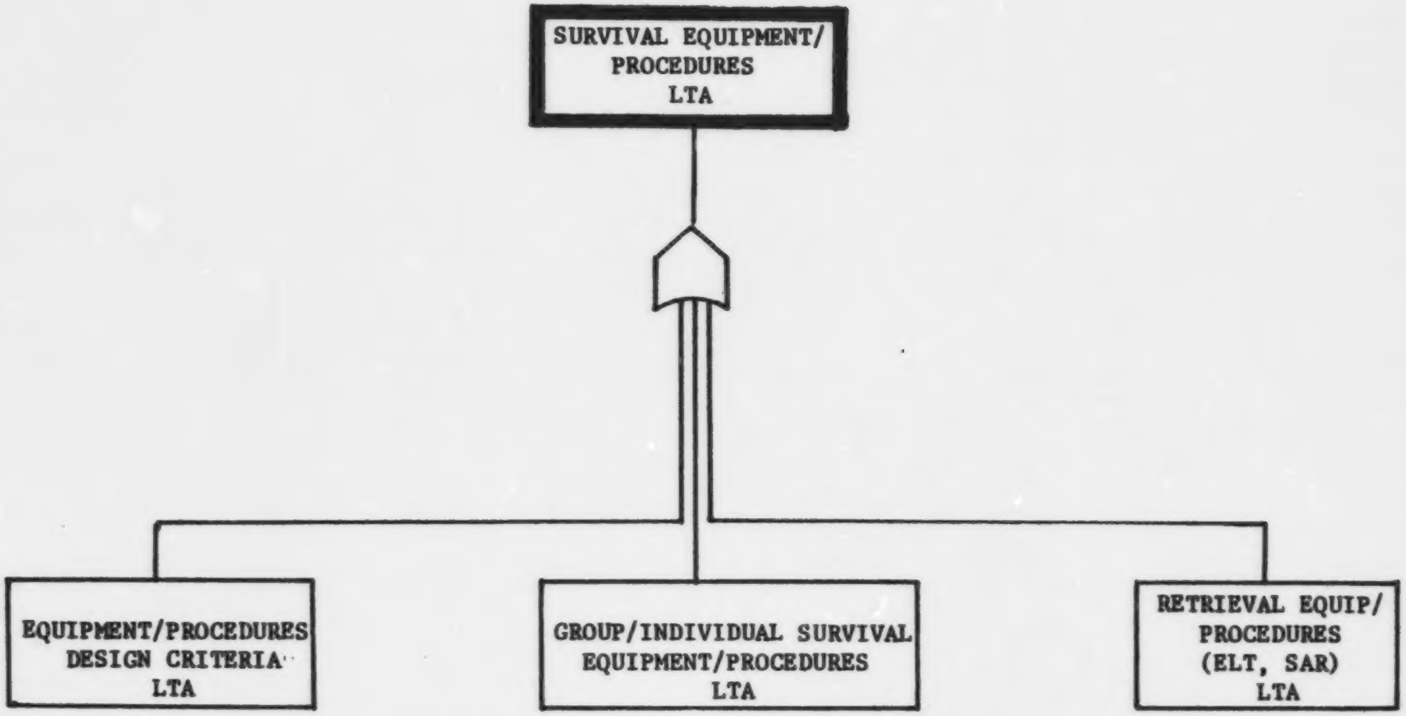

SURVIVAL EQUIPMENT/
PROCEDURES
LTA
EQUIPMENT/PROCEDURES
DESIGN CRITERIA
LTA
GROUP/INDIVIDUAL SURVIVAL
EQUIPMENT/PROCEDURES
LTA
RETRIEVAL EQUIP/
PROCEDURES
(ELT, SAR)
LTA

EXHIBIT 5.10 SUBPROBLEM ANALYSIS FOR PRIMARY PROBLEM AREA "SURVIVAL EQUIPMENT/PROCEDURES LTA"

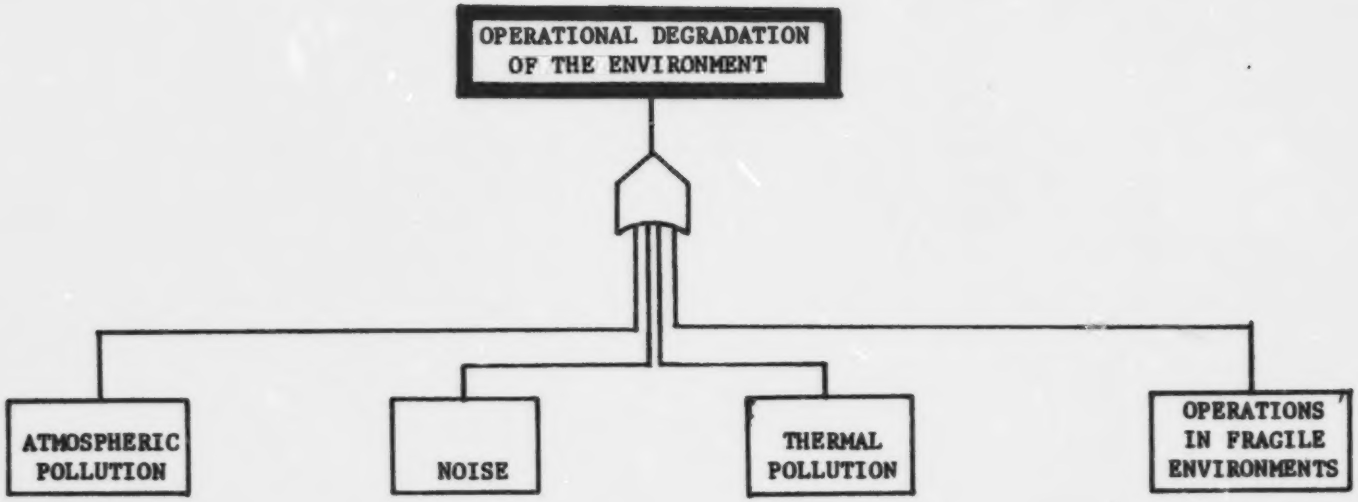

OPERATIONAL DEGRADATION OF THE ENVIRONMENT
ATMOSPHERIC POLLUTION
NOISE
THERMAL POLLUTION
OPERATIONS IN FRAGILE ENVIRONMENTS

EXHIBIT 5.11 SUBPROBLEM ANALYSIS FOR PRIMARY PROBLEM AREA "OPERATIONAL DEGRADATION OF THE ENVIRONMENT"

APPENDIX A

RESULTS OF FACT-FINDING

APPENDIX A

RESULTS OF FACT-FINDING

Appendix A documents the investigations carried out with respect to the manner in which safety R&D is being performed in the various jurisdictions, both in Canada and the United States. These findings are based on steps 1-4 of task 1 of the detailed work program. This chapter, together with chapter 1, constitute the output of step 5 of this first task. Findings are based on an extensive review of the available literature (cf. selected bibliography in Appendix A), and a large number of interviews with government officals both in Canada and in the United States, with transportation safety managers, safety professionals and academics. A complete listing of interviewees, together with summary notes of interviews, and our interview format document, may be found in Appendix B.

The appendix roughly follows the structure of the report outline agreed during the progress review meeting of February 2, 1983. A general overview section will be followed by sections devoted to the individual transportation modes of air, road, rail, marine and multimodal transportation respectively.

A.2 General Overview: United States

A.2.1 Safety R&D Approaches

In general, the United States and more specifically the Department of Transportation (DOT) in that country, is a number of years ahead of Canada in terms of the attempts it has made in developing some rational framework, method or process, for identifying R&D needs (including safety R&D needs). Unfortunately, however, most of these attempts have remained barren for political/institutional reasons, and at the present time, only one Administration of DOT, the Urban Mass Transportation Administration (UMTA), has been able to implement any kind of satisfactory solution to this problem.

A.2.2 The Institutional Framework

It is most important, if not decisive, to understand the institutional (including the political/institutional) framework for decision-making. In both Canada and the United States, this is a historical development. In the United States, the DOT was established as a result of the U.S. Department of Transportation Act of 1966 (49 USC 1651) which provides as the overall mission of the Department, "to assure the coordinated, effective administration of Federal transportation programs and to develop national transportation policies and programs conducive to the provision of fast, safe, efficient and convenient transportation at the lowest cost consistent with other national objectives, including the efficient utilization and conservation of the nation's resources". Safety is thus one of four major mission elements.

However, as we have already noted, it is not an easy task to separate a particular mission (in this case safety) from other departmental missions. However, in a 1972 study*, an attempt was made to allocate the budget for 1973 over the safety-related mission elements and programs. Results were as follows:

	Percent for Safety
National Highway Traffic Safety Administration (NHTSA)	100%
Federal Aviation Administration (FAA)	93%
Coast Guard (USCG)	60%
Federal Railroad Administration (FRA)	43%
Federal Highway Administration (FHWA)	28%
Office of the Secretary (OST)	7%
Urban Mass Transportation Administration (UMTA)	2%
St. Lawrence Seaway Development Corporation (SLSDC)	N/A
Total DOT	39%

Unfortunately, the study did not estimate what portion of total safety dollars was attributable to safety R&D.

The top safety spender was the FHWA which received 70% of DOT's 1973 Budget Authority and accounted for 44% of its safety dollars. The FAA was next (17% of the budget and 37% of safety dollars) followed by the Coast Guard (9% and 13% respectively). More recent figures are not available but the ranking probably still holds, (with the exeption of the Research and Special program Administration (RSPA) which was established in 1977). The current program missions for R&D in the various administrations are as follows:

- National Highway Traffic Safety Administration (NHTSA) - administration of programs related to safety performance of motor vehicles, drivers, and pedestrians, and programs for reducing economic losses from crashes and repairs; administration of the Federal odometer law and the national maximum speed limit; and promulgation of average fuel economy standards.

- Federal Aviation Administration (FAA) - regulation of air commerce to foster aviation safety, promotion of civil aviation and a national system of airports, achievement of efficient use of navigable airspace, and development and operation of a common air traffic control and air navigation system.

- United States Coast Guard (USCG) - marine environmental protection, commercial vessel and recreational boating safety, port safety, security, search and rescue, aids to navigation, ice operations, military readiness, and enforcement of laws and treaties.

---

* DOT. "Allocations for Safety: FY1973 Estimated Budget Authority", Nov. 15, 1972.

- Federal Railroad Administration (FRA) - development of a national rail policy, administration and enforcement of rail safety laws and regulations, administration of financial assistance programs, revitalization of the Northeast Corridor rail service and operation of the Alaska Railroad.

- Federal Highway Administration (FHWA) - coordination of the total operation and environment of the highway system with particular emphasis on improvement of highway safety.

- Urban Mass Transportation Administration (UMTA) - assistance in the development of improved mass transportation facilities, equipment, techniques and methods; promotion of the planning and establishment of areawide urban mass transportation systems; and assistance to State and Local governments in financing such systems.

- Saint Lawrence Seaway Development Corporation (SLSDC) - development, operation and maintenance of the part of the seaway between Montreal and Lake Erie, within the territorial limits of the United States.

- Research and Special Programs Administration (RSPA) - performance of research, analysis, and technical development for DOT with emphasis on pipelines safety, transportation of hazardous cargo, safety, security, and multimodal research and development.

Under DOT's corporate philosophy, each Administrator reports directly to the Secretary and has total responsibility for his/her modal areas. All R&D efforts within the Department are mission oriented, but the users of the programs are diverse. The USCG and FAA are their own users of the developed technologies and information, while NHTSA's R&D program supports its regulatory responsibilities. In contrast, State and local governments and motor carriers are the primary beneficiaries of FHWA R&D programs. UMTA's R&D programs are targeted towards assisting urban and local transit system operators, and FRA supports the railroad industry. RSPA supports the Department, the public, industry, regional, State and local governments and is its own user in the hazardous materials and pipeline safety regulatory areas. R&D efforts within SLSDC are primarily aimed at improving the efficiency of its own operations.

A.2.2.1 Safety R&D

Safety R&D is not given any formal priority, nor is it treated or administered separately from other forms of R&D. However, it does appear to have a higher profile under this administration. (Reagan administration)

A.2.2.2 Planning, Programming and Management of R&D

Research and Development is considered to be an activity undertaken in support of policies and programs established to promote the missions of the respective administrations and of the DOT as a whole. In effect, it is a mission-oriented support activity which is performed:

- To stimulate technological advances in transportation. This is performed and managed by RSPA, especially in cases where there is no other operating administration in the Department to conduct R&D, in intermodal and transmodal transportation, as well as R&D that relates to the transportation system as a whole.

- As a basis for sound regulations. This kind of R&D is performed within the various operating administrations in direct support of their missions and functions.

- To improve the effectiveness of Federal grants. This is also carried out by the several operating administrations. However, federally sponsored research in highways is also managed by State governments and by the Transportation Research Board.

- In direct support of departmental operational missions such as at FAA and the Coast Guard.

Prior to 1977, Departmental R&D policy and oversight responsibilities were assigned to the Assistant Secretary for Systems Development and Technology (TST). TST's assignments resulted in a Departmental R&D management system, which, until TST's dissolution in 1977, provided for program reviews, resource analyses and monitoring of two or three dozen key R&D projects. In addition to its Office of the Secretary (OST) staff function, this office performed some multimodal research, as well as some occasional modal research (e.g., the supersonic transport).

The first attempt to come to grips with the problem we are now facing in Canada was initiated by this office through a 1973 program under PPA OS 447, "DOT Transportation Safety R&D Program Investigation". Its mandate was "to develop a background of safety-related R&D data, to conduct studies of critical safety issues, and to recommend a balanced program which provides the highest possible return on the safety R&D investment".*

During the mid-1970's, the Office of University Research , which was part of TST at the time, also commissioned a number of studies in an effort to adapt and apply the concept of systems safety to the transportation industry, with mixed results. A probabilistic systems methodology for the quantitative risk assessment of existing and also future transportation systems was developed. A systems safety methodology was also adapted for use in the planning, design and operation of new transportation systems (all modes). However, no attempt was made to apply systems safety to assist in establishing the R&D needs of the DOT as a whole or in measuring the effectiveness of existing R&D programs.

The Office of System Development and Technology was abolished in 1977, and since that time, policy guidance and planning of R&D at the Departmental level has been inconspicuous at best. The Assistant Secretary for Policy and

---

* David S. Glater and Nancy Accola "Review of Safety Related Statutory Authority administered by the Department of Transportation." Transportation Systems Centre Report No. DOT-TSC-OST-73-45. Prepared for the Office of the Secretary, Office of R&D Policy, October 1973.

International Affairs is responsible for performing R&D policy planning and long range planning of the national transportation program, and supporting the DOT operating elements in the planning of their modal programs. Safety R&D policy planning is currently performed in this office by the Industry Operations and Safety Division of the Office of Industry Policy (Chief: Eloise Brooks).

The Assistant Secretary for Budgets and Programs conducts some review of R&D programs, specifically the larger projects. Technology sharing and information dissemination is performed by the Office of the Assistant Secretary for Government Affairs.

In general, however, R&D (including safety R&D) planning and project selection, programming (including resource allocation) and evaluation activities, originate within the eight operating administrations, with only a loose overall coordination at the top (Office of the Secretary). The process is thus highly decentralized.

A.2.3.1 Future Plans and Prospects

A "Research and Development Policy Statement of the Department of Transportation" was issued by the DOT in January 1981. (This followed completion of a DOT Task Force analysis of "Research and Development Activities in the Department of Transportation and Selected Federal Agencies" published in December 1981.) This policy statement called for the establishment of an Office of Research and Technology in the Office of the Secretary which would be responsible for translating secretarial goals and objectives into R&D priorities. A Research and Technology Advisor will be responsible for coordinating the development of an annual R&D priorities document to provide guidance to all elements of the Department in the development of their own reserch agendas, Spring Preview and R&D budget submissions:

- The agenda's annual update of research priorities will reflect changes in national needs and policy objectives within the context of a stable, developing program.

- The agendas will provide a basis for departmental review of modal R&D objectives and planned initiatives to assure that the total DOT program is coordinated and prioritized.

- Development of these research agenda documents will support and precede the budget and related processes, to assure that R&D objectives and needs are specified annually.

Coordination of the departmental R&D priorities document will be a joint effort with the Assistant Secretaries for Policy and for Budget and Programs, with ongoing assistance from a departmental advisory group composed of a representative from each operating administration. The document will be submitted to the Secretary for his approval and transmittal to the administration in January, in ample time to be integrated into other departmental management processes. The figure opposite indicates several sources of input to DOT R&D initiatives, which will be received by the R&T Advisor, and demonstrates how the R&D policy-planning process will tie into the Department's annual planning-budget cycle.

The operating administrations will continue to be responsible for the planning, funding, management and performance of R&D in support of their missions and functions while the R&T Advisor will be responsible for overall R&D program coordination and oversight. The diverse roles and responsibilities of the operating administrations include establishing their research agendas (i.e., establishing modal goals, objectives, and priorities) and providing the resources needed to accomplish their missions. The strengthened structure and process needed to effect the coordination and management of departmental R&D will not, however, centralize R&D activity at the expense of undermining the work of the operating administrations. The operating administrations are considered to be more familiar with their relevant operational environments, in closer contact with the potential user community, and have the advantage of technical expertise to better evaluate R&D needs and priorities; they are also in a better position to involve potential users in their R&D programs through their advisory committees.

The above proposal is still active although the Office has not yet been created. According to Eloise Brooks (Office of Industry Policy), the present Administration is not expected to move too quickly in this matter.

A.2.4 R&D Project Selection and Evaluation

The principal management process for resource allocation and prioritization at the Administration and Departmental levels is the budget process. Two separate issues are involved in project selection and budget allocations for R&D (including safety R&D) within the DOT:

- allocation of Departmental R&D budgets among administrations;
- project selection within the modal administrations.

A.2.4.1 Departmental Allocations

In principle at least, mechanisms exist within the budgeting process which would allow the Secretary of Transportation (OST) a measure of discretion in the allocation of Departmental resources to R&D. However, it must be remembered that public or Congressional visibility and opinion may make it difficult to change the orientation of Departmental efforts. Furthermore, many R&D programs are ongoing by nature.

Project selection is done initially within the modal administrations. Projects are then grouped into R&D budget decision packages, which are eventually ranked within the Zero based budgeting (ZBB) submissions to OST. This ranking, thus, reflects the judgmental analysis of the modal administrators. Within OST the budget process provides for interrelating the R&D packages of the various administrations. Based upon staff advice and his own views, the Secretary can make changes in the ranking; hence, the apportioning of funds between or among administrations.

A.2.4.2 R&D Project Selection by Administration/Mode

As already indicated, the Office of the Secretary (OST) does not normally perform a project selection or initiation role. Its role is the more passive one of approval (or disapproval, program adjustment, etc.) and oversight of selected activities (e.g., the Transportation System Acquisition Review Council (TSARC) and Program Monitoring and Evaluation System (PMES) processes).

Each administration makes an attempt to prioritize their R&D projects, including safety-related R&D projects. All projects begin with the definition of a need, but how this need is defined and where the need originates tends to differ from one administration to the next. For example, projects are developed within the Coast Guard mainly in direct response to specific requests made by the non-R&D program managers (Rear Admiral level, reporting to the Commandant) responsible for major mission areas; in other administrations the projects are proposed less formally to the head of its R&D unit, who develops an overall program subject primarily to review of the Administrator and higher approving levels. Despite such stylistic differences, there are several aspects common to all DOT administrations.

- Projects are developed to satisfy needs within the agency mission and goal structure.

- Crises, such as transportation disasters, can provide rapid stimulus for specific new projects. Congress or public groups often maintain pressure until completion.

- The agency R&D program is formulated and coordinated by an R&D office.

- The R&D portion of the agency budget provides form and visibility for higher level review of plans.

- Each administrator is responsible for the makeup and performance of his/her R&D programs.

Not much in the way of formalized process or "methodology" is in place in any of the Administrations to "assist in establishing research and development needs and provide a measure of the (safety) improvements achievable through R&D". However, in the safety area, a possible exception to this is the Urban Mass Transportation Administrations (UMTA). In the mid-70's, they commissioned a study which was performed by the Institute of Safety and Systems Management at the University of Southern California, Los Angeles. Entitled " Safety Program Plan Development of the Office of Safety and Project Qualification", the work was completed in 1977, and is currently in use. It is a planning tool for all safety programs at UMTA, not only safety R&D programs.

Other Administrations have made attempts to introduce a formalized methodology for assisting in establishing R&D needs, but for political or institutional reasons, they have not been adopted. The Federal Highway Administration (FHWA) commissioned a study in 1973 which was undertaken by Stanford Research Institute under DOT Contract No. FH-11-8095. Completed in 1976 and entitled "A Rational Determination of Priority Targets for R&D", the methodology proposed a systematic (though not a "system safety") methodology which was accepted but never implemented. This was complemented by a "National Highway Safety Needs Report" prepared by Research Triangle Institute in 1976.

In addition, the National Highway Traffic Safety Administration (NHTSA) has recently developed (in-house) a method of determining its own safety priorities. A safety priority plan has been prepared on this basis, but has not yet been accepted. The method is not based on a "systems safety" approach, but rather on analysis of "human harm", which is quantified as a cost-weighted sum of the number of people injured or the number of injuries sustained, either fatal or otherwise.

In summary, "systems safety" is only one of a number of approaches that have been tried towards developing a methodology for targeting R&D (including safety R&D) program needs. These approaches may be classified as follows:

- congressional and political priorities and pressures (all-pervasive);

- managment, commitee or "panel of experts" consensus (common in all administrations);

- "systems safety" approach (UMTA);

- "portfolio management" approach (FHWA but not applied);

- cost-effectiveness approach (NHTSA, USCG and FAA).

Clearly, the "systems safety" approach may only be applied in situations where safety R&D has been functionally and administratively separated out from R&D in general. This can only be done in certain specific institutional settings such as UMTA and NHTSA. As already indicated, "systems safety" has traditionally been used as a management rather than as a planning tool (except to the extent that planning is a part of management). This too is only possible however in cases where the management in question is in a position of control over all parts of the "system" throughout all the phases of the life cycle (e.g., as achieved at the Department of Defense* or at NASA). This is partially the case at UMTA but not at NHTSA which has little control over systems design, construction, operation, maintenance, etc.

A.2.4.3 Monitoring and Evaluation

DOT does have a formal Program Monitoring and Evaluation System (PMES) which has been used to evaluate certain major safety R&D programs (e.g., NHTSA's Research Safety Vehicle Program). In general, however, the individual modal administrations perform this task in-house through a variety of methods. A good idea of the methods applied may be gleaned from the following documents.

- Federal Aviation Administration (FAA)

  -Batelle Columbus Laboratories. "Evaluation of Safety Programs with respect to the Causes of Air Carrier Accidents". Report No. ASP 80-1, January 1980.

---

* cf. DOD System Program Requirements Standard MIL-STD-882A.

- Batelle Columbus Laboratories. "Evaluation of Safety Programs with Respect to the Causes of General Aviation Accidents". 2 vols. Report No. ASP 80-2, May 1980.

- National Highway Traffic Safety Administration (NHTSA)

- J.A. Croke. Management and Evaluation Handbook for Demonstration Projects in Traffic Safety. U.S. Dept. of Transportation. Report No. DOT-802 -196.

- Highway Safety Research Institute. "Funding for Highway Safety Reseach, Development and Demonstration in the National Highway Traffic Safety Administration". Report No. UM-HSRI-79-88. (PB 80137672).

- Arlene M. Cleven and Joseph T. Fucigna. The Evaluation of Highway Traffic and Safety Programs. Dunlop and Associates Inc., Darien Conn. 1976.

- Transportation Research Board, Commission on Sociotechnical Systems, National Research Council. Transportation Systems Safety and Project Analysis. National Academy of Science, Washington, D.C., 1979.

- U.S. Department of Transportation. Office of Programs and Demonstration Evaluation, National Highway Traffic Safety Administration. Effectiveness and Efficiencies in Traffic Safety Programs - Overview. Technical Report No. DOT HS-806-130 (PB 83 109637).

- U.S. Coast Guard

- U.S. Department of Transportation, U.S. Coast Guard. Cost, Benefit and Effectiveness of the Merchant Marine Safety Program. Washington, D.C., 1968.

A.2.5 Conclusions of Relevance to this study

The U.S. experience in the application of logical methods or processes to assist in the establishment of R&D needs of government, demonstrates above all else the importance of political and institutional realities. Little success has been achieved by these methods south of the border precisely because they ignored the overriding weight of congressional pressures (the "critial event syndrome") on the one hand, and internal political and institutional jockeying on the other ("institutional feasibility"). In fact the biggest planning problem, is how to structure the motivations of program managers so as to obtain the best problem solution rather then the best personal solution.

Management decisions are typically influenced by such considerations as:

- career advancement. Defensibility is often more desirable than soundness;

- standard modes of functional behaviour based on organizational inertia;

- preference to limit analysis to technical disciplines and professional experience with which managers/professionals responsible are familiar.

Ways must thus be found of coordinating and integrating:

- the motivational factors driving the decision-makers;
- functions and career patterns within bureaucracies;
- the technical disciplines applied.

A major problem is that choices tend to be distributed over an agency rather than focussed in a single key decision-maker. The National Science Foundation's (NSF) Technology Assessment and Risk Analysis (TARA) Group gave some attention to these problems during a NSF sponsored conference on Risk Management at Boston University Law School on February 17-18, 1983.

This all suggests that the implementation process is as important (if not more important) than the "system" itself, and must also include the necessary institutional arrangements needed to make the methodology work in practice.

The lesson for the conduct of further work on the present study would seem to be that we should be most sensitive to these factors in the Canadian context, and spend more time reviewing the attempts that have been made in the United States, more specifically at the DOT, with somewhat less attention being given to the mechanics of "systems safety" as a technical approach to implementing safety.

A.3 General Overview - Canada

A.3.1 The Institutional Framework

The Transport Canada program mission is "to attend to the development and operation of a safe and efficient national transportation system that contributes to the achievement of government objectives, and to operate specific elements of this system".

The Department's strategic objective in safety is one among nine strategic objectives which are met through the various departmental policies, strategies and programs. In this respect, the Department is charged, "to ensure an adequate level of safety is provided for the national transportation system".

Air Administration services include air traffic control, airways, aeronautical information, meteorological services, search and rescue, accident investigation, airport security, telecommunications, air carrier and airport inspection, and airport emergency services. Regulatory activities include the issuing of licences to individuals and equipment certification based on the meeting of certain conditions. Most of these are safety-related.

Marine Administration services include aids to navigation, ship movement systems in controlled areas, pilotage, accident investigation, search and rescue, icebreaking, ship inspection, cargo inspection, pollution control assistance and port security. Regulatory activities include the issuance of ships' and officers' safety certificates.

Surface Administration activities include the development of production standards for new vehicles and tires which are regulated to ensure product safety. Investigations by Transport Canada officials are made for a variety of motor vehicle accidents. Extensive testing of vehicles and tires takes place, and major public education safety programs have also been undertaken.

Other government agencies also have responsibilities for transportation safety. In the rail mode, equipment standards and operating rules are administered by the CTC, who conduct accident investigations. The department liaises with the CTC on rail safety matters affecting policy advice to the Minister and administers grade separation and railway relocation programs. While highways are a provincial responsibility there is a substantive federal role in product testing and a federal-provincial cooperative objective to attain a substantial reduction in motor vehicle fatality rates. Many aspects of transportation safety are self-regulated in that carriers themselves ensure a high degree of safe operation, both to satisfy their customers and to reduce their costs of insurance. This applies in all the modes: air, marine, rail and highway.

While safety is a primary mission responsibility, there is no clear-cut division between programs and activities which are safety related and those that are efficiency related. A recent study by the Strategic Planning Group* draws attention to this problem by recognizing the tripartite nature of safety within departmental planning and programming as follows:

- Level of safety for facilities/services where safety is an output measure of a transportation activity or a criteria by which the system is assessed based on an objective of operational efficiency. A level of safety is sought and achieved but safety is not intended to be the basic objectives of the activity. It is not a safety activity but rather a transportation activity of which level of safety is a necessary attribute.

- Safety Activities. Activities where safety is a primary objective rather than a performance measure.

- Support activities such as data, planning, R&D, accident investigation and safety analysis which support the achievement of the first two types of safety.

The most common form of departmental program or program activity is the first, where funding is decided on criteria other than safety, and where safety is often traded off against other objectives. Transport Canada does have certain activities whose primary purpose is transportation safety, but these are much less common. Research and Development in safety is identified as a support activity (as in the United States).

---

* Transport Canada. "Transportation Safety Analysis of Strategic Change: an appraisal study. Systems Planning Directorate, Strategic Planning Group, November 1980.

It is impossible for these reasons, to determine what portion of the Departmental budget allocation is attributable to safety related programs and activities, or even to R&D support activities in the field of safety.

A.3.2 Planning, Programming and Management of R&D

The Departmental planning framework is a top-down process which devolves from strategic planning through medium-term programming to operational planning and evaluation. Planning is required among other things to provide guidance in setting priorities for resource allocation. Programming is the process of allocating resources to activities in order to achieve departmental objectives. A programming schedule of events begins 21 months before the fiscal year for which resources are allocated via Main Estimates, as shown below*:

Strategic Planning Guidelines (SPGL)	June 30
Group Planning Memoranda Reviews (GPM)	Mid Nov.
Preliminary Program Forecast (PPF) Submissions	January
Initiation of Strategic Overview	January
Program Forecast and Strategic Overview completed	March
Approval-in-Principal (APD) and Program Approval (PAD) Documents	Ongoing

This cyclical resource planning process reflects ongoing planning activities within each of the department's 4 Programs which respond to priorities of the current and proceeding years editions of the SPGL. At the same time, the resource planning process takes account of the specified resource targets in dollars and person-years in the preparation of GPM, PPF and PF documents in that cycle.

Strategic Planning Guidelines are completed 21 months in advance of Main Estimates. This document, prepared by the Strategic Planning Group provides guidelines for the forthcoming programming cycle and serves as the initiating document for this process leading to the preparation of the program forecast. Group Planning Memoranda represent the modal planner's response to the SPGL within the programming cycle. The SPGL also provides an ongoing reference point for specific projects, studies, and program approval documents, referred to as APDs and PADs.

The APD is the vehicle by which Approval-in-Principal is sought from management early in the program cycle for a proposal developed in response to anticipated needs or demands. The APD is tentative and preliminary in nature as it represents future resource requirements as yet only broadly defined. Major alternatives, including approximate costs and benefits, form part of the APD submission, along with relevance to departmental policies. The PAD is the vehicle by which program approval is sought from management for a proposal developed in response to anticipated needs or demands. It is the final stage of departmental approval, and represents a fully-defined, mature project, containing a clear and logical justification for the proposal, including the results of any special studies, quantitative and qualitative data, technical feasibility, cost and expected benefits and a thorough financial analysis.

---

* Transport Canada, Op cit.

In the departmental Program Activity Structure the four departmental Programs are divided into a logical set of activities. It is this strucutre through which resource requirements are estimated, programmed and allocated. Research and Development support activities are part of this structure and process of resource allocation.

A.3.3 R&D Project Selection and Evaluation

The budgeting process is the chief tool for the allocation of research and development funds to the operating Administrations of Transport Canada. The actual process of project selection and evaluation within these bodies has traditionally made use of the modal R&D Advisory Boards, originally conceived in 1972. The Rail Advisory Committee was constituted in 1974. A Marine Advisory Board was established in 1977 and separate Air and Highway Advisory Boards followed in 1978.

The purpose of these Boards is to provide advice to the various Administrations on the planning and implementation of technology R&D, on programs and projects needed by industry and to provide a forum for the exchange of information and an interface with other government departments and with industry. They are charged among other things with developing a multi-year research program for government and recommending program priorities for R&D. Work is conducted by committees charged with specific tasks. For example, the structure and objectives of the various Committees of the Marine Transportation Advisory Board are as follows:

- Vessel and Systems Technology: To develop technology to improve design, operation and construction of vessels, on the basis of economics, fuel consumption, to meet the specific Canadian environment, and to secure the capability of export.

- Terminal Operations & Shore Facilities: To develop technology to improve the intermodal transfer of cargo from ship to shore, on the basis of safety, economics, and to meet the specific Canadian environment.

- Navigational Aids & Traffic Management: To develop technology to assist the passage of vessels in confined, coastal and ice-infested waters on the basis of economics, safety, and maintaining a satisfactory environment.

- Ice Management: To develop technology to study and apply the physical and chemical properties of ice and its effect on structures; to provide data for improved design and operation of vessels and fixed structures.

- Marine Statistics & Data: To develop and make available information to upgrade the techn logical knowledge of the industry.

- Steering & Policy: To provide guidance and advice on Board matters relating to the Board's functions and activities. (Comprises Board Chairman and Committee Chairmen only.)

Ad Hoc Committees may also be established to develop proposals related to specific subjects not falling into any of the above.

In the field of evaluation, the Safety Programs Evaluation Project Committee of the Roads and Transportation Association of Canada (RTAC) has recommended an approach to the economic evaluation of transportation safety programs*. It is of course primarily highway oriented.

A.4 Current Practices in Aviation Safety

A.4.1 Introduction

The aviation and aerospace sectors of transportation are key to the extent that they have pioneered many (if not most) of the safety optimization philosophies, approaches, techniques and disciplines now current in the other modes. In addition to systems safety, examples would include human factors research, including flight simulation, crash-fire and crash-worthy design technology, failure effect and reliability analysis, quality assurance and design reviews, and of course the techniques of accident investigation. The Aviation Safety Technology Program of the National Aeronautics and Space Administration (NASA) in the United States for example, has as its objective, "to provide, through a continuing program of basic research and system technology, for the development of improved safety technology, improved knowledge of aviation meteorology, and improved aircraft systems operational reliability and efficiency". NASA is currently active in the area of atmospheric hazards research, fire technology, structural crash-worthiness technology, critical operating factors definition, simulations and flight data reconstruction, and development and implementation of the Aviation Safety Reporting System (ASRS).

The Federal Aviation Administration (FAA) of the U.S. together with the Canadian Air Administration of Transport Canada, co-operate in and take advantage of many of these programs. The FAA is currently drafting a "National Airspace System (NAS) plan for Engineering and Development" in support of FAA programs in the fields of airborne safety, aircraft safety, aviation medicine and continuing regulatory activity. In Canada, the Air Administration of Transport Canada is preparing to establish new administrative structures to implement a National Air Transportation Safety Plan (NATSP).

One reason for this state of affairs is the fact that aviation safety is more challenging technically and organizationally, than other transport modes. Jerome Lederer, the President Emeritus of the Flight Safety Foundation, Inc. has identified seven major "forcing functions" in support of this thesis**.

---

* Roads and Transportation Association of Canada. Guide to Evaluation of Safety Programs. Ottawa, 1981

** Jerome Lederer, "The Economic and Social Impact of Aerospace Safety". ICAO Bulletin, September 1976.

- Unlike ground transportation, an aircraft in trouble cannot stop. It is continuously combatting the unrelenting force of gravity which instantaneously takes advantage of any weaknesses or failures in the aircraft's battle for survival.

- Unlike other forms of transportation, it is three dimensional in operation, which creates problems involving control atmospheric variables and terrain.

- It is bedeviled by limitations of weight, space and energy requirements.

- Mistakes or failures, mechanical, structural or human, are more likely to be catastrophic than in any other transport activity.

- It requires the co-ordinated, co-operative, timely, more careful effort of a greater variety of personnel and associated facilities than any other system of transportation. The complex infrastructure involves airports, weather services, communications, traffic control, medical services, dispatching, training facilities, monitoring, incident reporting, etc.

- It encompasses many more scientific disciplines and technical variables than any other system of transportation.

- Air transportation is more sensitive to man-made safety problems than other systems of transportation.

It is also true, however, that the catastrophic results of aviation accidents guarantees a high media coverage which creates a public awareness and demand for a high level of Aviation safety. This in turn guarantees a high level of of funding at the political level. In the words of former US Transportation Secretary William T. Coleman, Jr., "when it came to research engineering and development money requests for the FAA, especially in areas involving safety, I had no problem with the Office of Management and Budget not going along with the proposals"*.

During our interviews, an official of the FAA confirmed that this is still true today, in spite of budget cuts in other areas.

A.4.2 The Management of Safety in Aviation

It is partly for the above reasons also, that the air mode has traditionally enjoyed a higher degree of international as well as national cooperation, coordination and control than other modes. The International Civil Aviation Organization (ICAO) and the International Air Transport Association (IATA) both came into being in 1945. For ICAO, the first objective as written into Article 44 of the Chicago Convention is to "ensure the safe and orderly growth of international civil aviation throughout the world", and at least sixteen of the eighteen subsequent annexes to this

---

* Aviation Week and Space Technology, February 7, 1977. p.56.

Convention are partly or wholly concerned with the problem of safety. On behalf of the airline community, IATA too is dedicated to promoting, "safe, regular and economical air transportation ...".

In the United States, the Federal Aviation Administration is charged with "regulating air commerce to foster aviation safety ...", and in Canada, the Air Administration has been given the mandate to develop a "... safe and efficient national civil air transportation system". In all cases, the mission of safety is the first of the several missions for which these various bodies are responsible.

The following provides greater detail on the safety mandates and functions of these agencies.

A.4.2.1 International Civil Aviation Organization (ICAO)

The role of ICAO is both regulatory and non-regulatory of international air transportation. On the regulatory side, it is concerned with building up a body of international standards, the Standards and Recommended Practices (SARP's) and the Procedures for Air Navigation Service (PANS). ICAO not only sets these standards, but is involved in a continual process of review, and also assists member states in implementing them.

ICAO also has a large non-regulatory role in the safety field. The ICAO Annex 13 on Aircraft Accident Investigation, the Manual of Aircraft Accident Investigation and the ICAO Accident/Incident Data Reporting System (ADREP system) are widely followed and used by member states, including Canada (though Canada does not make safety recommendations as required by Annex 13).

ICAO is strongly oriented to accident prevention. This is defined as "the search for detection and assessment of hazards and development of appropriate methods and recommendations and the taking of actions to minimize or eliminate accidents and incidents". The term hazard is defined as "any condition or circumstance having the potential to induce an aircraft accident or incident".

The 1979 ICAO Accident Prevention and Investigation Divisional Meeting, recommended the production of an ICAO Accident Prevention Manual (APM), the third draft of which is currently being reviewed by member states. The following are the main areas of discussion.

- historical trends;

- accident prevention concept;
    - nature of accident
    - system description
    - importance of human performance,
    - management responsiblities;

- roles and responsibilities for accident prevention;

- hazard discovery, evaluation

- safety measurement;

- hazard elimination;

- safety promotion.

It is interesting to note the stress placed on "incident" reporting, investigation and analysis. This parallels a recommendation of Dubin regarding the establishment of an incident data base. Incidents are similar to accidents in terms of the causal chains, but have no injury consequences. Incidents are thus fertile ground for hazard analysis because there are many times more incidents than accidents.

It is also interesting to note the emphasis on prevention of accidents rather than fatalities/injuries. Virtually, nothing is mentioned concerning survivability. This is perhaps the result of the higher chance that air accidents do involve fatalities/injuries.

In summary, ICAO's non-regulatory responsibilities include:

- outlining accident prevention concepts and providing guidance based on proven methods;

- establishing international procedures for accident investigation and reporting. (This is done through Annex 13 - Aircraft Accident Investigation, the Manual of Aircraft Accident Investigation and the Accident/Incident Data Reporting Manual (ADREP);

- disseminating accident and incident information through the ADREP system;

- undertaking specific safety studies using ADREP data.

In most States, the body responsible for civil aviation is charged with the responsibility for achieving a high standard of aviation safety. It undertakes this by formulating regulations and procedures based on ICAO SARPs. These are tailored to meet local environmental or operational conditions. Surveillance and inspection procedures are then used to ensure that the aviation community complies with the national regulations.

A.4.2.2 International Air Transport Association (IATA)

IATA is governed by a committee structure under the direction of an Executive Committee elected by the Chief Executives of member airlines. It has two main functional branches, the Technical Department and the Traffic Department. Safety is one of the two main missions of the Technical Department (along with efficiency), although the Traffic Department has also been involved in safety matters through a recent ramp safety promotion campaign.

The Technical Department and its six Regional Technical Offices work on behalf of the carriers in three main fields:

- establishing worldwide standards (e.g. of safety);
- planning facilities and services on a regional basis;
- implementing plans.

The Technical Department represents the interests of airlines at international forums and acts as a clearing-house of technical information on safety and other matters. The Department's activities are controlled by the Technical Committee with its six Advisory Committees as follows:

- Safety;
- Flight Operations;
- Airports and Terminals;
- Engineering and Maintenance;
- Communications;
- Medical.

These Advisory Committees all have some interest in safety. For example, the Flight Operations Advisory Committee has two sub-committees who have been very active in promoting safety. The Flight Crew Training Sub-Committee has sponsored a number of Flight Crew Training Meetings on the theme "Training for Safety". The Flight Simulation Sub-Committee is also very much concerned with safety issues.

The Engineering and Maintenance Advisory Committee (EMAC) has produced guidance material on such things as de-iceing procedures, design and maintenance against corrosion of aircraft structures, and on the maintenance and overhaul of aircraft. The Medical Advisory Committee has developed a medical manual in the area of aviation medicine, and a special Human Factors Working Group has developed a manual to acquaint flight crew with the role of the human operator in the man/machine/environment system.

IATA works closely with ICAO in representing the interest of the worldwide airline community in matters of direct concern, including safety in aviation.

A.4.2.3 Federal Aviation Administration (FAA)

The U.S. Federal Aviation Administration is charged with regulating air commerce to foster aviation safety; promoting civil aviation and a national system of airports; achieving efficient use of navigable airspace; and developing and operating a common system of air traffic control and air navigation for both civilian and military aircraft. The research and development activities of the agency are directed towards providing the systems, procedures, facilities and devices needed for a safe and efficient system of air navigation and air traffic control. The FAA is also involved in developing and testing improved aircraft engines, propellers and appliances. Safety research involving aircraft certification, improved fuel systems, flame resistant materials and the like reflects another important R&D responsibility.

It is evident that R&D at the FAA is conducted primarily in support of its own operations, air traffic control services in particular. The 1984 program budget for Research, Engineering and Development is distributed as follows:

	$ millions
Air traffic control	77.7
Advanced computer	156.6
Navigation	11.0
Aviation weather	14.3
Aviation medicine	6.1
Aircraft safety	17.8
Environment	2.4
Total	285.9

R&D in support of FAA regulatory responsibilities is concentrated in the area of aircraft safety. Almost all R&D must be classified as safety-related.

Major Program Thrusts

The FAA is currently conducting two major R&D program thrusts in the safety area, the National Airspace System Plan for Engineering and Development and implementation of the Aviation Safety Analysis System (ASAS).

The NAS Plan for Engineering and Development is the product of an extensive and ongoing review of research, engineering and development activities supporting the total FAA mission and the user community. The main objectives include:

- accomplishing the necessary research and development at the time it is required to support the implementation of the National Airspace Plan for Facilities and Equipment and Associated Development, designed to modernize the ATC system of the 21st Century;

- developing and testing of systems and procedures for the timely integration of advanced navigation techniques, so as to meet increasing demand and to allow airspace users to operate with a minimum of artificial constraints and with improved fuel efficiency;

- performing the research and development to improve airport capacity at major metropolitan airports and accomodate user requests with minimum constraint;

- developing systems, procedures and techniques to reduce the potential of injury or loss of life in aircraft accidents;

- performing the necessary research and development for weather data collection, processing and dissemination, providing near real-time and hazardous weather information leading to improved and efficiency of operation of the NAS;

- developing systems, methods and techniques to integrate and balance airborne and ground-based air traffic control systems;

- providing for research, development and testing of systems and procedures for further productivity improvements in air traffic controller, flight service specialist, and airway facilities maintenance work force performance;

- providing regulatory support through the use of laboratories (at the FAA Technical Center and at the Civil Aeromedical Institute), accomplishment of regulatory activities for aircraft certification, airframe and materials testing, and safety procedural regulations.

This R&D effort is thus designed to support all FAA programs, including the NAS Plan for F&E, the National Airports System Plan, the Rotorcraft Master Plan, the National Airspace Review (NAR) and the various regulatory support programs. It is expected that this R&D plan will:

- provide for timely completion of research and development activities supporting the implementation of the aforementioned programs;

- provide for further improvements in safety;

- provide for long range improvements of services while accommodating growth and diversity of aviation;

- provide for increased flexibility in the future use of airspace, with less interference to individual freedom of flight;

- provide for increased system capacities;

- provide for increased use of automation and application of advanced technology.

The FAA's safety programs stress accident prevention through hazard identification and control in the human, equipment, environmental and procedural areas. This objective can only be achieved however, as a result of actions taken on the basis of adeqate and reliable data. Information gaps in the area of safety have plagued the FAA for many years. It is not a question of shortage of data. In fact, aviation safety related activity produces over eight million papers of forms a year. However, this information is scattered in numerous incompatible systems of data, and does not provide the kind of information needed for hazard analysis and control.

The General Accounting Office in one of three major studies of the problem recommended that the FAA develop a more effective and timely system to address safety issues, and that it change the present system from a reactive to an anticipatory one. The Transportation Systems Centre subsequently developed a plan to collect, store and organize information into a single system called the Aviation Safety Analysis System or ASAS. One of the most important aspects of ASAS is the reorganization of all existing safety related data bases, and transfer to the central processing facility at Oklahoma City. New data bases will be established, and the necessary linkages between data bases will be established. Components of the system include the computer and communications hardware, software to link, manipulate and analyse the data, and the data bases themselves.

Among the many data bases which will be integrated into this system are the FAA Accident/Incident Data System (AIDS), the Service Difficulty Reporting System (SDR) and the NTSB Aviation Safety Reporting System (ASRS).

It is expected that ASAS will be fully operational by 1985.

Administration and Management of R&D

There is no comprehensive overall, long range plan for R&D, which would cover both ATC Systems safety (i.e. the NAS) and aeronautical flight safety activities. The need for R&D planning has perhaps been less acute at FAA than in other DOT Administrations, as a result of the generosity of Congress. In fact, R&D funding has increased from $67 million in 1982, $110 million in 1983 to a projected $286 million in 1984, mainly as a result of the NAS. The new Administrator, J. Lynn Helms, has been the main force behind the "planning" thrust of the NAS.

R&D Program Selection and Evaluation

R&D program selection is an informal process of consultation and peer group review. Most programs are on-going and are sold to the Administrator who then helps to sell them to the Office of Management and the Budget and to Congress. The FAA seems to operate fairly autonomously within DOT in this regard. The key is to have a strong Administrator behind the programs.

While no formalized process exists within the FAA with respect to the selection of Programs, this Agency has developed sophisticated methods for the evaluation of Programs, including safety programs (though not specifically safety R&D programs or activities).

Two studies are worthy of mention in this regard, both of which were undertaken by the Batelle Columbus Laboratories:

- Evaluation of Safety Programs with respect to the Causes of Air Carrier Accidents. Report No. ASP 80-1, January 1980

- Evaluation of Safety Programs with respect to the Causes of General Aviation accidents. Report No. ASP 80-2, May 1980.

The prime purpose of these studies was to determine the extent to which current FAA safety programs were aligned against the causes of air carrier accidents. The heart of this work was the development of a common dictionary of conditions/causes to which both the air accident data base (with considerable massaging) could be aligned, and to which the safety programs could also be allocated. Dollar weighting was also included on the accident side using a costing model and distributing over the causal factors. Time series data were generated for each set of data. The conslusions, for example in Air Carrier operations, were framed in terms of:

- mechanical safety programs: no change required;

- environmental (weather) programs: further research into the human factor/weather interaction;

- human factors programs: further initiatives are required to address human error problems in behavioural terms at the detail cause/factor level.

Note that, although directed to an evaluation of programs, this work did result in indications of areas of research need.

A.4.2.4 Canadian Air Transportation Administration (CATA)

Although no specific reference is contained in the Aeronautics Act with respect to aviation safety, CATA has a strategic objective "to ensure that an adequate level of safety is provided for the national air transportation system".

The following are the main organizations involved in the field of aviation safety:

- Aviation Safety Bureau (DAS): This Branch develops, co-ordinates and directs national investigation and analysis of civil aircraft accidents, incidents and aviation hazards. It also develops and provides a national program of safety information, education and motivation for the civil aviation community of Canada.

- Aeronautical Standards and Legislation (DSL) and Legislative Review Branches (DLR): These Branches are responsible for the development and maintenance of aeronautical standards and legislation and the air information service vital to the safe, efficient control of civil aviation in Canada. The senior Director (DSL) is also responsible for the Legislative Review Branch and is Head of the Aeronautics Act Task Force which currently is reviewing all aspects of aeronautics legislation, enforcement procedures and policies.

- Aeronautical Licensing and Inspection Branch (DLI): This Branch develops and implements policy, procedures and standards for all civil aviation personnel licensing. Specifically, its staff controls and develops aviation personnel examinations, flight training standards, and issues all personnel licenses; applies standards to domestic and national air carrier operations; and administers a licensing program of navigational and landing systems for national airports. DLI also produces policies and procedures for the enforcement of regulations, standards and directives.

- Airworthiness Branch (DAB): This Branch is responsible for the management of all airworthiness programs, approvals and continuing safety of all civil aeronautics products manufactured or operated in Canada, and the continuing airworthiness support for all Canadian manufactured aeronautics products in foreign countries.

These Branches all have a safety function. However, recent studies have pointed to lack of coordination of the various activities and an organization not ideally structured from a safety point of view. We return to this point again, below.

The recent Dubin Enquiry on Aviation Safety (released May 1981 to February 1982) dealt with the adequacy of federal law, regulations and rules and of practice and procedures governing aviation safety; the deficiency of enforcement; the airworthiness and maintenance of aircraft; the adequacy of aviation incident reporting and investigation, and aviation accident investigation. This has already resulted in the establishment of a separate Canadian Aviation Safety Board for accident/incident investigation and the recommendation of safety measures. Other organizational changes are also likely to result. In fact, almost all recommendations are being adopted by Transport Canada.

A Legislative Committee is currently redrafting the Civil Aeronautics Act and it is expected to result in the passage of a new Act 18 to 24 months hence with clear specification of powers and responsibilities.

Concurrent with the release of the Dubin Enquiry was the commencement of a safety initiative entitled "National Air Transportation Safety Plan". The objective was stated in September 1981 as:

- To develop a national civil air transportation safety plan for introducing a comprehensive planning process for identifying and addressing aviation safety issues.

The workplan had evolved to the following by late 1982:

- Review Existing safety information sources:
    - data bank inventory;
    - current system description and risks (historical accident rates);
    - identify data base deficiencies and propose remedies re ability to be used in "statistical inference modelling".
- Systems analysis of Safety Management structure:
    - develop a model and assess current system effectiveness of CATA.
- Develop event-tree procedures of key physical facilities:
    - adapt a model from Atomic Energy Control Board;
    - apply to high risk system.
- Time Line Analysis:
    - a "data" gathering prelude to Task 5, below;
    - break each component of the system description into time segments;
    - for vehicle, terminal, way systems.

- Specific System Simulations:
  - evaluate existing simulation models (FAA);
  - maintenance;
  - air traffic control at specific high volume terminals.
- Overview (model) of System Risk:
  - integrate the various approaches: historical data analysis, fault tree, safety organization, time line simulation;
  - to assess the impact of safety of expected/proposed design changes to the system.
- Risk management/policy development.

The initial NATSP workplan included a study of public attitudes and expectations in aviation safety, but this has been postponed to at least the completion of Tasks 1 to 7.

The current status of this workplan is completion of most of Task 4 and the initial stages of Task 5. Current funding levels run out with the completion of Task 5, expected in September 1983. A further funding proposal for Tasks 6 and 7 is being developed currently.

Some of the findings and results from this work include:

- systems descriptions for vehicle, terminal, ways (airspace);
- a list of 50 data bases related to safety maintained in CATA;
- the inadequacy of the Accident/Incident Data System (AIDS) with respect to casual factor chaining;
- the British are working on a standardized method to include an "event-tree" chain on each report for computer analysis;
- some investigation into the fact that the U.S. FAA has also catalogued about 60 data bases related to safety and is currently in the midst of a multi-million dollar project to integrate these data bases into a single Aviation Safety Analysis System (ASAS);
- safety management not a visible function in CATA;
- resource levels devoted to safety cannot be separately identified so no evaluation possible;
- a proposed functional safety organization model - not likely to be implemented on top of changes due to Dubin;

- modification and use of "event analysis" computer model originally used in atomic power plant design. A computerized model is needed due to the complexity of possible chains of events leading to an "accident" or undesired event;

- plans to simulate the air traffic control operations at Toronto to investigate under what conditions hazards arise.

There is currently a proposal to establish a new Directorate of Aeronautical System Safety Requirements (ASSR) which would incorporate ASA and ASP (from the Aviation Safety Bureau) and a new branch, Aviation System Safety Requirements, in permanent charge of planning NATSP.

With respect to the safety R&D planning process at CATA, the following observations may be made:

- from on organizational point of view, safety management has not been readily separate from other activities;

- within safety itself, interrelationships between programs dealing with different components of the air transportation system have not been identifiable;

- resource levels devoted to safety management have not been separately identified;

- research is certainly carried out, particularly in the "way" component, with the aim of identifying hazards and developing countermeasures. Hazards are deemed worthy of analysis/control if the probability of causing an accident is greater than one chance in a million. It is not clear how this probability is estimated in actual cases;

- there appear to be little ranking, or cost-benefit analysis to prioritize work on hazards. It would appear that interest groups and informed and expert judgement combine to result in a resource allocation;

- further to the above, many CATA officials do not distinguish the term, "Safety R&D". Rather, they think in terms of hazard identification and control using "engineering" solutions.

In summary, it would appear that safety R&D, using a broad definition is certainly an ongoing function in CATA. However, there is no central coordination and, further, no systematic process to identify and prioritize safety projects.

A.5 Current Practices in Road Safety

A.5.1 Introduction

In general, the road mode in most countries is less systems oriented then other modes, in particular air, mass transit and marine. This is primarily the result of the fragmentation of this mode, both from the jurisdictional point of view and from the point of view of its inherent characteristics.

Jurisdictionally, central government control of roads and road traffic in most countries is relatively weak compared to other modes. In North America, for example, federal governments have delegated a substantial degree of responsibility and power to other levels of government. In the United States, the primary responsibility for highway construction and policing falls to the States and municipalities. In Canada, this is the responsibility of the provinces and local government units. In the United States however, the Highway Trust Fund, established in 1956, provides the basis of Federal aid (and hence also some control) over States' highway programs and standards and in construction and improvement to the National System of Interstate and Defence Highways. Apart from the TransCanada Highway system which was funded in large part by the Federal government, this does not apply in Canada.

In effect, the jurisdictional situation is the antithesis of that of a missile delivery system for example, where management has total control over the entire life-cycle of the system from concept design through to mission accomplishment.

This is partly due to the vary nature of the "system" of road transportation. The guideway is shared by a large number of different vehicles, each controlled by operators with varying degrees of education and skill. The vehicles themselves are manufactured and assembled independently of the rest of the "system" and the guideway controls are embryonic when compared to other modes (e.g. air traffic control).

The span of control over the system tends to determine the degree of emphasis that is placed on accident prevention as opposed to accident protection. In a missile delivery system, the accent is exclusively on accident prevention (system reliability) which is achievable through a systems safety approach. In the road transportation environment, emphasis tends to shift towards accident protection. However, even for road safety programs oriented towards accident prevention, the systems safety approach is difficult to apply for the jurisdictional and other reason already given. Programs are generally designed around one aspect of the system (e.g. the "human factor" or highway geometry), generally that aspect over which a particular agency has jurisdication.

These considerations are reflected in large part by the policies and programs of the jurisdictions covered by our investigation as described below.

A.5.2 International Agencies

The Organization for Economic Co-operation and Development (OECD) Road Research Programme has conducted numerous studies in the area of road safety for many years. Until recently however, research has tended to concentrate on one area at a time such as alcohol, roadside obstacles, child safety, etc.

In 1982, it was decided to establish an ad hoc group under the joint leadership of the United States and The Netherlands to develop a conceptual framework for an integrated safety program, based on a multi-disciplinary approach in many fields. This group, known as the High Level Group S1 on

Concepts and Methodologies for Integrated Safety Programmes had its first meeting in Washington, January 13-14, 1983. Objectives of this work are as follows:

- Develop typical causal chains leading to road accidents and identify the scientific and technical fields in which expertise may help to improve safety performance.

- Catalogue and assess research findings from experiments, field tests, controlled demonstration projects and documented behavioural studies in key safety areas, such as law enforcement, education, etc., in order to develop an array of measures found to be effective in various safety areas.

- Develop linkages, preferably in matrix form, between problem areas in road safety and optional safety programmes, taking account of a programme's expected effectiveness, cost, administrative complexity and public reaction. Based on the relationship suggested by the matrix, (where possible) review conceptual management techniques by which safety measures addressing multiple problem areas can be identified.

- Identify, in some detail, future research needed to advance the concept and development of integrated, multi-disciplinary road safety programmes.

A report outline was agreed to and member countries were assigned responsibilities for individual chapters. Canada has the lead role in the the work of Chapter VII - Management Factors and Strategies, which will:

- address the decision-making process;
- consider how to integrate levels of decision-makers and disciplines;
- consider management of co-ordinated research;
- provide examples.

The Road and Motor Vehicle Traffic Safety Branch of Transport Canada (DTS) will be responsible under Mr. S. Chris Wilson.

In addition, OECD, in conjunction with the European Conference of Ministers of Transport (ECMT) and the Transport and Road Research Laboratory of the U.K., sponsored a World Conference on Transport Research in April 1980 during which traffic safety was a major theme. The following countries provided details of techniques used in the planning of and evaluation of road safety programs.

Japan: An Analysis of Traffic Accidents for making National Safety Policies
U.S.S.R.: Systems Analysis for Traffic Safety Problems.
France: Securité routière et planification des transports.
Hungary: Traffic Safety Research and Activity in Hungary.

These papers are contained in Volume 4 of the Proceedings of the World Conference on Transport Research, London, 14-17, April 1980*.

In the United Kingdom, the Transport and Road Research Laboratory used a multi-disciplinary team to identify the main contributory factors and their interactions for about 2,000 accidents which ocurred in the early 1970's. The team attended the scene of the accidents, conducted interviews and held team discussions. This enabled them to calculate a distribution of accidents over:

- road user factors
- road environment factors
- vehicle factors

in order to calculate actual risks. A further study was done to link countermeasures and target groups of accidents to assess the potential for reduction of risk (damages) due to accidents.

A.5.3 United States

The DOT is vested with the authority and duties contained in two major acts relating to motor vehicle safety; the National Traffic and Motor Vehicle Safety Act of 1966, and the Highway Safety Acts of 1966 and 1973. The Secretary of Transportation delegates responsibility for the first of these Acts, and for those portions of the Highway Safety Act dealing with motor vehicle and traffic safety, to the Administrator of the National Highway Traffic Safety Administration. For those portions of the Highway Safety Act dealing with the safety of the guideway portion of the highway system, responsibility is delegated to the Administrator of the Federal Highway Administration.

National Highway Traffic Safety Administration (NHTSA)

NHTSA is charged with the responsibility for setting and enforcing motor vehicle and equipment safety performance standards, including tire and bumper standards, providing grants-in-aid to States which develop acceptable highway safety programs, and conducting safety related studies to investigate or review:

- the use of mass media, especially the licenced broadcast media, to inform the public of accident reduction techniques. The Secretary is specifically directed to develop a series of short highway safety television programs;

- methods for encouraging greater citizen participation in highway safety, with emphasis on law enforcement and accident detection and reporting;

---

* cf. Transport Research for Social and Economic Progress. J. Stuart Yerrell (Ed.) Vol. 4. Proceedings of the World Conference on Transport Research, London, 14-17 April 1980.

- pedestrian and bicyle safety including States and local regulation and enforcement, the relationship between alcohol and pedestrian and bicycle safety, and an analysis of bicycle and pedestrian safety funding allocations;

- States' highway safety needs and the cost of meeting them;

- establishement of the "National Center for Statistics and Analysis" to handle accident data and standardize accident reporting.

In the specific area of R&D, research, development, and demonstration projects are commissioned or conducted in-house. In order to develop safer motor vehicles and equipment, the NHTSA has been involved in conducting research, testing, development, and training, including the collection of data and the procurement of experimental vehicles and equipment. Research necesary to development bumper standards that will provide for damageresistant safe passenger motor vehicles has also been undertaken.

NHTSA is also authorized to use general highway research funds for safety research, which may include research on highway safety systems, vehicle and driver characteristics, accident investigations, communications, emergency medical care, and transportation of the injured. Research funds may also be used for grants for training of highway safety personnel, for research fellowships, and for traffic and motor vehicle safety demonstration projects.

Examples of such R&D would include: the effect of drug use on highway safety; the characteristics of driver performance; and the effectiveness of driver training programs.

NHTSA safety programs fall into two main categories, those related to the driver and vehicle occupants and non-occupants (e.g. pedestrians), characterized by the term highway safety programs, and those related to the vehicle itself, characterized as motor vehicle safety programs.

More important from our point of view, programs are also classified as crash prevention or crash protection programs. In the highway safety area for example, driver training and alcohol-related programs are aimed at prevention, whereas safety belt and child restraint programs are aimed at accident protection. A similar division in the motor vehicle safety area is apparent between e.g. the use of daytime running lights (crash avoidance) and vehicle crashworthiness programs such as frontal impact protection (crash protection).

NHTSA is currently engaged in a major review of its planning priorities. This is geared to safety programs rather then safety R&D programs, R&D being a support activity to the programs themselves. A cost-benefit methodology has been developed, based on data files maintained by the National Centre for Statistics and Analysis (NCSA), such as the Fatal Accident Reporting System (FARS), the National Accident Sampling System (NASS), and more particularly, the National Crash Severity Study (NCSS). The methodology first calculates the human harm resulting from fatalities and degrees of injury severity, and then develops programs based on the potential for harm reduction of alternative courses of action. Cost effectiveness of alternative programs and ranking of priorities is achieved by setting the harm reduction against the costs of the program. This method was first applied in the area of crash protection and subsequently extended to crash prevention program priorities as well*.

A draft planning document on Safety Priorities has been prepared by the Office of Plans and Programs of NHTSA, but had not yet received the blessing of the Administration as of April 1983.

Federal Highway Administration (FHWA)

The FHWA provides the necessary financial assistance to States for construction and improvements to the National System of Interstate and Defense Highways and for urban and rural transportation programs. (Authorization for 1983-86 have been provided through the 1982 Surface Transportation Assistance Act). It also administers those portions of the Highway Safety Acts dealing with "highway safety programs, research, and development relating to highway design, construction, and maintenance, traffic control devices, identification and surveillance of accident locations, and highway-related aspects of pedestrian safety". The FHWA also shares responsibility for the elimination of railroad grade crossing hazards with the Federal Railroad Administration (FRA).

Safety is an integral part of all FHWA programs. However, certain programs are more obviously safety-related then others. For example, the Motor Carrier Safety Program is designed to reduce the risk of accidents in truck and bus highway transportation by regulating motor carriers in interstate commerce. The Railroad-highway crossing demonstration projects are obviously safety-related. The FHWA also provides highway-related safety grants to the States as well as Motor Carrier Safety grants to enforce commercial motor vehicle safety standards.

Highway safety research and development program funds are used to identify, correct and evaluate critical elements that contribute to loss of life, disabling injuries, and property damage on the highways. A total of $12.3 million is budgeted for this activity in February 1983. Appropriations are made out of the Highway Trust Fund.

In the mid 1970's, the FHWA did make an attempt to develop a methodology to assist in establishing research and development priorities. This effort was not specifically directed of safety-related R&D, but rather to the R&D effort in the FHWA as a whole.

A study was commissioned from the Stanford Research Institute, Menlo Park, California, and completed in December 1976. Entitled, "Rational Determination of Priority Targets for Research and Development", the study provided guidelines for the establishment of R&D priorities at the FHWA based on an investment portfolio approach. Although applied to several R&D projects on a test basis, it was never implemented, for political and institutional reasons. However, it does provide viable guidelines for conducting decision analyses of R&D projects and establishing R&D priorities.

---

* cf. A.C. Malliaris, Ralph Hitchcock, and James Hedlund, "A Search for Priorities in Crash Protection". Paper presented at the Society of Automotive Engineers' International Congress and Exposition, Detroit, February 22-26, 1982.

Attempts were also made in the mid-70's to introduce the concepts of systems safety to the highway mode, based on studies conducted by the Polytechnic Institute of New York. They apparently fell on deaf ears*.

The FHWA also co-operated with NHTSA in preparation of the 1976 National Highway Safety Needs Report which was the first concerted attempt by the DOT to identify highway safety needs and develop a prioritized list of counter-measures. Thirty-seven known counter-measures were ranked by decreasing potential to forestall fatalities on a nationwide basis. The costs of implementing each counter-measure were also estimated and the cost effectiveness ($ per fatality forestalled) for each was calculated and ranked. Although caveats were expressed regarding data and methodological deficiencies, it became clear that some powerful conclusions could be reached. For example, cost effectiveness ranged from $506 for mandatory seat belt usage to $7,680,000 for roadway alignment and gradient (on a per fatality prevented basis). These kinds of differences likely outweigh any data deficiencies. It also became clear that in the face of limited funds, there is a lower practical limit to the level of fatalities.

FHWA is currently working with several states, including Alabama, Michigan, North Carolina and Utah, to link roadway, pavement and bridge inventory files with traffic volume, accident records and other files, in one comprehensive data file known as the Safety File Linkage Demonstration Project. The objectives are to:

- develop a work plan for linking multiple highway information files;
- develop and test software for linking the files;
- conceptualize and develop a file format for an intersection/interchange file;
- prepare a user's manual.

This program effort is similar in purpose and scope to the FAA Aviation Safety Analysis System (ASAS) already described.

A.5.4 Canada

In Canada, jurisdiction of the road mode is divided between Federal and Provincial modes.

A.5.4.1 Canadian Surface Transportation Administration (CSTA)

At the Federal level, CSTA, as the administrator of the Motor Vehicle Safety Act and the Motor Vehicle Tire Safety Act, is primarily responsible for new vehicle and tire standards and regulations. The line operations involve conducting inspection and testing to monitor compliance, and evaluation of vehicle technology and regulations (often) developed in other countries.

---

* cf. E.J. Cantilli, M. Horodniceanu and L.J. Pignataro. "System Safety: a New Approach to Traffic Safety". Traffic Engineering, December 1976

For the Road and Motor Vehicle Safety Branch of CSTA, the primary driving forces for R&D are vehicle and tire standards. Nevertheless, they have been conducting and sponsoring research in the human factors area although this appears to be primarily within the jurisdiction of the provinces. Although the federal mandate in this area is not clear, it is expected by some provinces that there should be federal leadership.

CSTA is now in the first phases of a major study involving criteria for vehicle occupant injury. This work has been precipitated by a set of new U.S. standards. The work will involve analysis and testing regarding how occupants receive trauma during an accident. The first phase ($900,000) involves frontal impact. This research is undertaken to develop an evaluation to ensure the adequacy of the U.S. standards.

CSTA is also continuing with research to develop an understanding of human performance under the interaction of alcohol and marijuana. This work is not directed at any particular counter-measure, but is basic in nature.

CSTA has also just initiated a two year study ($214,000), jointly funded with the FHWA, entitled "Decision Analysis Techniques in the Evaluation of Safety Counter-measures". The basic principle underlying the evaluation technique is that many counter-measures that could give a 5% or 10% improvement (a significant improvement) are not found effective using standard statistical hypothesis testing. That is, the null hypothesis of no effect will not be rejected, given the small sample sizes in much counter-measure research. An example is the enforcement of speeds limits.

It is contended that, while it is clear that lower speed reduces accidents (and fatalities/injuries), it has never been shown, over many studies, that speed limit enforcement measures actually affect individuals' choices of driving speeds.

The statistical technique proposed in this study is Bayesian (likelihood) analysis. This technique has the ability to embody all relevant research to the present and to furnish the decision-maker the result in proper form. The technique apparently can also assist in putting a value on proposed R&D in terms of the likelihood of gaining incremental knowledge. This could potentially assist in the allocation of resources to R&D projects.

The present study will attempt to apply these methods to six selected counter-measures and the previous accumulated research results on each.

In discussion with CSTA, the planning techniques are fairly pragmatic for identifying and prioritizing safety R&D projects. As noted above, research in vehicle standards flows naturally from other off-shore work. In evaluation of some counter-measures, the first step is to identify a target sub-group of accidents and then review the data. Typically, the data are inadequate so that research and physical test designs are required.

Two or three years ago, CSTA conducted a Delphi consensus panel of management to identify and prioritize R&D requirements. Subsequently, the top choices were adopted, and have, to some extent, influenced budgets and research efforts. This process can, however, to some extent be influenced by the political/public pressure process, resulting in a short-term view of priorities. Thus, long-term basic research would likely not be identified or given priority.

A.5.4.2 Provincial Jurisdiction

The Provincial governments have jurisdiction over the other major components of the system related to safety as follows:

- driver licencing and inspection;
- vehicle licencing and inspection;
- enforcement (especially truck weights/sizes/goods);
- motor carrier licencing;
- dangerous goods waybill system;
- road/highway construction and signing.

In some cases, the provincial governments have a sizable number of professionals devoted to safety issues and management, particularly Alberta, Saskatchewan and Ontario. Enforcement officers may be federal (RCMP), provincial police, or municipal police.

A.5.4.3 Associations, Foundations, Councils

In Canada there are a number of organizations which have a safety mandate. We interviewed officials in a number of them, including:

- Canada Safety Council (CSC);
- Traffic Injury Research Foundation (TIRF);
- Canadian Automobile Association (CAA);
- Motor Vehicle Manufacturers' Association (MVMA);
- Canadian Urban Transit Association (CUTA);
- Science Council of Canada (SCC);
- Ontario Motor Coach Association (OMCA);
- Canadian Trucking Association (CTA);
- Roads and Transportation Association of Canada (RTCA);
- Ontario Truck Safety Commission (Prof. Uffen).

Detailed interview notes for most of the above are contained in Appendix A.

Although each interview is interesting on its own, we have tried to distill the various comments as follows:

- very few do original/basic research. The exception is TIRF;

- most do secondary report/data gathering to assist in developing positions for their memberships and for safety promotional purposes;

- safety issues of interest develop through a process of reaction to public/media attention and survey of members;

- the CMVA safety expertise is supported by individual companies' extensive safety research organizations;

- OMCA says bus safety not an issue but SCC has just published summaries of (Swedish) research showing that rear-mounted engines are a safety hazard;

- truck safety - no adequate data; a major concern is increasing truck size/decreasing car size both due to a fuel economy motivation. Transportation of dangerous goods is the major safety issue for CTA;

- in truck and bus, it is said that 90% of accidents are the result of human factors;

- TIRF does original research. Most funding is from the government (CSTA). However, the research is driven by political pressures and although the research is original, it is not basic, in the sense of pure investigative long-term safety research. TIRF also maintains its own accident data base (100% sample of seven provinces since 1973). The primary source for this is coroners' records including police reports, inquests (if any), and toxicology reports.

- it appears that, in Canada, no one does the long-term safety research noted above, whereas, in the United States there are many such institutions;

- a major lacuna is the lack of adequate data relating casual chains/factors to accident results. It seems that funding agencies are not willing to devote resources for this purpose. It was suggested that specialized studies should be instituted to go after specific data requirements.

A.6 Current Practices in Rail Safety

A.6.1 Introduction

The present section will describe current practices in three fields of rail safety:

- rail intercity services;
- rail commuter services;
- rail transit services.

Rail intercity services are primarily rail freight services, whereas rail commuter and rail transit services are primarily oriented to the carriage of passengers.

Most railways and transit operators recognize safety as a fundamental element of sound railway operations and devote considerable management attention to the problem. For example, both CN Rail and CP Rail have Accident Prevention Programs and maintain computerized accident reporting systems which permit systematic, detailed analysis of the causes of accidents. The Association of American Railroads (AAR), through its Safety Committee, has always been heavily involved in rail safety. Throughout North America, track, cars, switches and controls are all designed to ARR standards.

The same applies to safety appliances on equipment and to handrails, footrails and similar facilities in stations and yards.

In Canada, the railways typically report to a number of organizations with interest in safety, including:

- Union international des chemins de fer (UIC) in Paris*;
- Association of American Railroads (AAR);
- Federal Railroad Administration (FRA) in Washington;
- Statistics Canada;
- Labour Canada;
- Railway Transport Committee (RTC).

This data is generally not compatible, since each organization has different reporting requirements (e.g., different thresholds for reporting an. accident)

In North America as in most countries, regulation of railways is largely a federal responsibility. The relevant bodies are the Federal Railroad Administration (FRA) and the Urban Mass Transportation Administration (UMTA) in the United States, and the Railway Transport Committee (RTC) of the Canadian Transport Commission (CTC) in Canada. Details are as follows.

A.6.2 Federal Railroad Administration (FRA)

The FRA is currently responsible for the regulation of U.S. intercity rail and also commuter services. It currently performs the functions previously carried out by the Interstate Commerce Commission (ICC) and the Commerce Department (High Speed Ground Transportation). U.S. and Canadian railways operating in the United States are required to make monthly accident reports to the FRA who may investigate serious acidents and report thereon.

Under the Federal Railroad Safety Act of 1970, the FRA is authorized to prescribe regulations and standards for all areas of railroad safety and to conduct, or contract out for necessary research, development, testing, evaluation of data and personnel training. The safety mission of the FRA was considerably enhanced by Section 16 (c) of the Federal Railroad Safety Authorization Act of 1980 which called for the submission to Congress of a System Safety Plan relating to the activities of the DOT in carrying out rail safety laws. Apart from the Northeast Corridor Improvement Program (which is now drawing to a close), grants to Amtrak (the biggest item in the FRA budget by far) and settlements for Conrail, the work of the FRA is almost exclusively safety oriented.

Research and Development is funded largely through the Contractual Support and Railroad Safety Programs. Contractual Support includes policy support, R&D support and special projects sub-programs, including equipment and track safety testing in support of FRA safety regulatory functions (Office of Research and Development). Railroad Safety includes funds for implementation of the System Safety Plan (Office of Safety).

---

* The equivalent organization in the transit field is the Union internationale des transports publics, located in Bruxelles.

The Office of Research and Development is functionally divided into Track and Equipment R&D program elements. Safety and cost-effective performance are the two main objectives. For example, the goal of the Improved Track Structures Research Program is the safety and cost effective performance of the track system as affected by maintenance and rehabilitation.

The FRA R&D Office has not developed any comprehensive methodology to assist them in identifying R&D needs as a whole. However, they have developed a formalized technique for identifying needs and prioritizing programs and sub-programs in the specific area of track system performance (the safety area was handled by means of an informal committee structure through the Transportation Systems Centre). Two studies were commissioned, the first by the MITRE Corporation (which looked at track rehabilitation-oriented R&D) and the second by Parsons, Brinckerhoff, Quade and Douglas, Inc. (maintenance- oriented R&D). The two studies were subsequently integrated*.

The methodology essentially involves a process of weighting of selected cost and benefit criteria by a committee of experts who then rank the sub-programs according to quantitative values (which also incorporate a probability of success factor).

The Office of Safety at the FRA is charged with the task of developing the overall plan in the safety area (which would necessarily impact R&D in safety), the System Safety Plan. The goal of this plan is to reduce accidents over the period 1982-1987 by 20% in each of the following priority areas:

- hazardous materials releases;
- serious passenger train accidents;
- railroad employee casualties;
- rail-highway crossing accidents;
- trespasser fatalities.

The effectiveness of the plan relies on a cooperative and coordinated effort involving industry, labour and government, technical research in safety related areas, specific performance standards of key FRA managers, and a yearly National Inspection Plan for railways.

The Plan was developed without the assistance of any formalized management decision process.

The Office of Safety is also the custodian of the FRA Rail Accident/Incident Data Base. Details are published in the monthly Accident/Incident Bulletin.

---

* cf. The MITRE Corporation, Track Rehabilitation and Maintenance Research Requirements. Report No. FRA/ORD/-80/09, Washington, January 1980.

A.6.3 Urban Mass Transportation Administration (UMTA)

The Urban Mass Transportation Administration is charged with the development of mass transportation (rail and bus), encouragement of the planning and establishment of area-wide urban mass transportation systems, and assistance to State and local governments in financing such systems.

UMTA provides both formula and discretionary capital and transit operating grants to State and local agencies. Capital expenses include construction, acquisition, modernization, and improvement of existing facilities and equipment, deployment of new technology and technical planning assistance. UMTA also provides research and training grants and contracts for the purpose of developing, testing and demonstrating new facilities, equipment, techniques, and methods (analytical, operational and managerial), and improving mass transportation services. Although is not a regulatory agency, this funding authority gives UMTA considerable (if not overhelming) leverage with the management of urban mass transportation properties, system developer and the equipment supply industry. For example, transit authorities cannot get federal funding unless they develop and implement a systems safety plan, based on guidelines established by UMTA as a result of a study undertaken by the Batelle Columbus Laboratories*. These guidelines are designed to show operators and supplier firms ways of setting logical safety goals and of establishing engineering procedures and the necessary organizational structure needed to implement them. In effect they provide a model for industry management and for basing the interaction, regarding safety, between pertinent Government agencies and the transit community.

The UMTA Office of Safety and Product Qualification (now the Safety and Security Office) also developed a specific "systems safety" methodology to identify critical safety issues for the agency, and to develop a safety plan for the work of UMTA itself. This methodology was developed by the Institute of Safety and Systems Management at the University of Southern California. Entitled "Development of a Safety Program Plan for the Office of Safety and Product Qualification" (two volumes, September 1977), it developed six keys objectives in the safety area, twenty nine critical objectives and over ninety specific objectives. Sixteen programs were subsequently identified and recommended for top priority consideration.

This work is the only successful use of systems safety concepts in the development of an R&D planning methodology in a government agency (a similar study performed for the U.S. Coast Guard was never used). Of all the DOT agencies, UMTA is perhaps the most progressive and aggressive in promoting the systems safety concept for the elimination or control of hazards in the field of transportation.

A.6.4 Canadian Transport Commission (CTC)

The CTC, and more specifically the Railway Transport Committee (RTC) of the CTC, is charged with the responsibility of supervising, regulating and

---

* cf. Batelle Columbus Laboratories, Safety in Urban Mass Transportation: Guidelines Manual. Prepared for the Office of Research and Development, UMTA, Washington, May 1975, Report No. UMTA RI-06-0005-75-2. (Batelle also produced a Research Report, April 1976, Report No. UMTA-RI-06-0005-75-3)

and investigating the Railways under the Railway and National Transportation Acts.

This control extends over the areas of railway operations (including safety), fare setting, construction and abandonment of lines and discontinuance of services, and the construction and maintenance of stations and other facilities.

In the area of rail safety, some confusion still exists between the jurisdiction of the CTC (primarily over derailments, collisions and rail-highway crossing accidents) and the Department of Labour (rail employee accidents). Thus, for example, employees in shops, stations, in track work groups etc. are all covered by Labour Canada. In the yards, the men in the ground are covered by Labour Canada, the men of the engine by RTC. If a brakeman gets off the engine to throw a switch, he is covered by Labour Canada. Any employees on a train are covered by the RTC, whether in the loco cab or in the caboose. If a track work gang is going to the work site in trailers or flat cars the gang is covered by the RTC. Once the men are at the work site, they are covered by Labour Canada.

The RTC administers the Uniform Code of Operating Rules (UCOR) issued under section 228 of the Railway Act. In 1974, under General Order No. 1974-1Rail, the CTC issued the present consolidation of regulations for the transportation of dangerous commodities by rail (the Red Book). The Railway Act (section 225) also requires all accidents involving injury or a given level of property damaging to be reported to the CTC. (This information is maintained by the Safety Section of Safety and Services Branch). Accident investigations may be initiated by one or more RTC officers, or a full scale inquiry may be instituted such as the recent Grange inquiry into the Mississauga derailment.

The first major inquiry was the General Safety Inquiry of 1971, established as a result of three serious accidents in 1970. The problems posed by the carriage of dangerous goods prompted the establishment of a Task Force on the Carriage by Rail of Dangerous Commodities which reviewed the hazards attendant on the carriage of these goods and evaluated safety measures. Its work was subsequently taken over by the Dangerous Commodities Technical Committee and the Railway Safety Advisory Committee. Additional activities undertaken by the RTC include review and improvement of track and railway maintenance standards, computerization of the accident/incident data base, and co-operation with the Railway Association of Canada (RAC) in the Lifesaver Program to reduce rail-highway crossing accidents.

On the other hand the RTC has no technical research capability. The CTC has a Research Branch, but this is more concerned with socio-economic research then technical research. The RTC might do a statistical study of accidents, for example, but they have no technical expertise or facilities.

Research undertaken for the RTC tends to be farmed out to TDC or to the National Research Council. For certain types of accident investigation (e.g., analyzing a broken journal) they might approach the Ontario Research Council.

The RTC do not budget for reseach or set priorities. They tend to react to accidents. For example, they commissioned studies on tank car metallurgy and the placement of horns on diesel locos. Both of these grew out of accidents. The result in each case was that the problem was referred back to the AAR for further investigation and revision of AAR standards in these areas. When a problem like this comes up, the money is simply found somewhere within the Commission to pay for the necessary research.

With respect to the Grange Commission inquiry, RTC staff reportedly agree with some recommendations, but not with others. They have asked Transport Canada to look into colour-coding of tank cars. This has to be consistent with U.S. practice. They have also directed the railways to carry out tests on mirrors. There tests have been completed, although it is uncertain at this time whether the RTC will actually order the installation of mirrors.

Transport Canada has established a Committee to deal with the Grange recommendations. They are reportedly investigating the potential of aluminium extrusion tank car liners to prevent explosions.

A.7 Current Practices in Marine Safety

A.7.1 Introduction

Two developments of recent years have tended to focus attention on the problems of marine safety. In the first place is the fact that the ocean is not expanding in width and depth to suit the growth in size and quantity of the world fleet. As vessels grow in size and speed, and above all in draught, they become increasingly confined to narrow channels and fairways which cramp their motions, degrade their steering and lesson the scope for collision- avoidance manoeuvres. The second problem arises from the size and physical/ chemical characteristics of the cargoes carried. A collision involving say a LNG carrier and a passenger ferry or the sinking of a large oil tanker could have consequences undreamed of a generation ago. The new factor here (and this is common to rail as well as marine) is the growing involvement of innocent third parties whether directly (one can think of the Halifax ship explosion of 1907) or indirectly through environmental damage (e.g., a major oil spill).

For these reasons, marine safety activities tend to become polarized between activities directed at accident prevention and those related to emergency response to catastrophic events. At the national level, this polarity is reflected in the thrust of major program activity and in jurisdictional distinctions among organizations dealing with emergency response and search and rescue, and other groups involved in marine safety (commercial ship safety and the safety of pleasure craft) and marine law enforcement (e.g. Coast Guard, RCMP, etc.). The application of systems safety approaches and techniques of safety management and risk analysis have been used by the marine industry for the evaluation of specific ship systems or sub-systems, but according to one authority, "for purposes of general Coast Guard regulations, too many different ship design and operating environments are involved to make those methods economically feasible"*.

---

* John S. Gardinier, "Towards a Science of Marine Safety". Paper delivered at the Symposium on Marine Traffic System (Advances in Technology session) The Hague, 11-14 April 1976. (Mr. Gardinier is Chief, Office of Research and Development, U.S. Coast Guard.)

The present description of current practices in marine safety does not cover the rather special problems of fishing safety or the safety of oil rigs and attendant service operations. Furthermore, while it does not cover Emergency Response or Search and Rescue (SAR) operations as such, it does take into account SAR safety and SAR prevention activities aimed at improving safety measures to prevent the occurrence of distress situations. Accident prevention and SAR prevention are of course analogous to the extent that resources dedicated to both activities may be traded off against the resources required for SAR (and other emergency response) operations.

Details regarding marine safety activities at the international and national levels are given below.

A.7.2 The Intergovernmental Maritime Consultative Organization (IMCO)

IMCO is the specialized agency of the United Nations established to deal with matters affecting safety at sea. Its prime objective is to facilitate cooperation among governments on technical matters affecting shipping and to ensure the highest possible standards of safety at sea and of efficient navigation. It is at once a platform and forum through which governments can express their views and also the international agency by which mandatory safety regulations, and other recommended practices and codes may be standardized and implemented throughout the world.

A number of these have come into force in recent years including:

Title	Year in force
Safety of Life at Sea 1948	1952
Safety of Life at Sea 1960 (various amendments pending)	1965
Safety of Life at Sea 1974	Pending
Prevention of Collisions at Sea 1972	1977
Prevention of Pollution of Sea by Oil 1954 (various amendments pending)	1954
Prevention of Pollution by Ships 1973	Pending
Load Line Convention 1966	1968
Intervention in Oil Pollution Casualties 1969	1975
Intervention in Pollution other than Oil	Pending
Civil Liability for Oil Pollution Damage 1969	Pending
Civil Liability for the Carriage of Nuclear Material 1971	1975
Compensation for Oil Pollution Damage 1971	Pending
Safe Containers 1972	1977
International Maritime Satellite Organization 1976	Pending
Procedures for Control of Ships 1975	Pending

An international Dangerous Goods Code has been issued and in 1973, the IMCO Assembly adopted a resolution relating to the safe carriage and handling of dangerous goods in port areas. IMCO is currently working on a hazard recognition scheme as a standard medium of information, and the UN is endeavouring to harmonize regulations of the movement of goods for all transport modes. (A UN numbering scheme for each subtances is in preparation).

A.7.3 United States Coast Guard (USCG)

The United States Coast Guard is responsible among other things for "the promotion of safety on and over the high seas and waters subject to the jurisdiction of the United States" (14 U.S.C. #2). Duties include administering laws and promulgating and enforcing regulations to promote the safety of life and property; establishing, maintaining and operating aids to navigation, ice breaking facilities, and search and rescue facilities. The USCG is also the agency charged with enforcement of U.S. legislation enacted pursuant to the various IMCO Conventions. It is involved in both commercial vessel and recreational boating safety. In addition, the Marine safety Council acts as a deliberative body to consider proposed safety regulations etc.

In the specific area of research and development, the USCG has the authority to:

> "conduct experiments, investigate, or cause to be investigated, plans, devices, and inventions relating to the performance of any Coast Guard function and co-operate and coordinate such activities with other Government agencies and with private agencies" (14 U.S.C. #93(d)).

The USCG R&D Support Program was established in 1969, primarily for the purpose of supporting the various operating programs of the Agency. Currently, however, the Office of Research and Development is somewhat more oriented to the support of the USCG regulatory programs. The main program activities of the USCG, together with the budgeted R&D Support for the February 1984 budget proposal is as follows:

Program	Budget Total	R&D
Search and Rescue	$ 436 million	$ 5.8 million
Aids to Navigation	$ 370 million	$ 3.1 million
Marine Safety	$ 128 million	$ 4.6 million
Marine Environmental Protection	$ 159 million	$ 6.8 million
Enforcement	$ 359 million	$ 1.0 million
Ice Operations	$ 57 million	$ 0.2 million
Military Readiness	$ 85 million	$ 0.6 million
Administration	$ 94 million	--
Total direct program	$1,688 million	$22.0 million

Much of this R&D effort is related to safety. In the specific area of marine safety, research is largely in support of regulatory programs. Emphasis is being directed towards crew/passenger safety and exposure to hazardous cargo vapours in the marine environment. In the area of marine environmental protection, emphasis is being placed on the enhancement of detection, identification, and quantification of pollutant spills, and development of new systems and procedures for the control and cleaning of these spills.

The establishment of a planning methodology to assist in establishing R&D needs in the safety area was actively investigated by the USCG in the mid-seventies. A study was commissioned from the Batelle Columbus

Laboratories and completed in May 1977. Entitled RDT&E Plan for Marine Safety, this report documented what was essentially a "system safety" method of identifying research needs in the areas of both marine safety and environmental protection. The study combined the research needs of all the Coast Guard's organizational sub-divisions relating to marine safety and environmental protection into a single, integrated plan of action. Fourteen project areas were identified, each addressing a major problem in marine safety such as "vessel collisions" or "identification of pollution spills". Project areas were subsequently subdivided into projects and individual tasks.

Unfortunately, this study did not sufficiently take into account the political and institutional realities of management decision-making in the Coast Guard and was therefore never implemented. It does however, provide a useful model for a logical "system safety" approach to hazard identification in the marine environment.

A.7.4 Canadian Marine Transportation Administration (CMTA) and the Canadian Coast Guard (CCG)

The Canadian Marine Transportation Administration (CMTA) formulates and implements marine policies and programs and is responsible for the operational, developmental and regulatory activities of Transport Canada in support of marine transportation and the development of ports and marine commerce in Canada. In addition to the office of the Marine Administrator, CMTA includes the Canadian Coast Guard (CCG) and six Crown corporations, including the Canada Ports Corporation, the St. Lawrence Seaway Authority, and the four regional pilotage Authorities. The CMTA, like the Air and Surface Administrations, is charged with ensuring an adequate level of safety, in this case in the area of marine transportation. While all the operating elements of CMTA have a safety responsibility, this mandate is carried out more specifically by the Canadian Coast Guard (CCG) which will be the focus of attention here.

The CCG is responsible for the following major program missions:

- Aids to Navigation: This program involves the provision of fixed and floating aids to navigation to mark channels, harbour entrances, prominent landmarks and obstructions: radio location sytems for the guidance of ships at sea; and navigable channels for the passage of marine traffic.

- Ship Movement Systems and Services: This program involves the provision of marine traffic management systems, safety and commercial communications facilities, and information services.

- Icebreaking, Arctic and Other Ship Support: This program involves the provision and operation of coast guard ships, facilities and services for safe and expeditious movement of marine traffic in ice covered waters; prevention of flooding on the upper St. Lawrence River; northern settlement resupply; the provision, operation and maintenance of ships including the vessel "MV Arctic" and services in support of other departments and agencies.

- Marine Search and Rescue: This program involves the provision and operation of facilities and services primarily used to detect distress and prevent loss of life where possible in the marine environment and to promote boating safety through educational and volunteer services.

- Regulatory: this program involves the development, administration and enforcement of marine, telecommunications and traffic management regulations and standards; the registration, licensing and inspection of ships, air cushion vehicles and cargoes; the examination and certification of marine personnel; the investigation of shipping casualties and crew accidents, and provision of prevention programs, the provision of pollution cleanup and other emergency services; and the administration of the Navigable Waters Protection Act.

All programs have a safety component. However, safety-related program activities tend to be focussed in the following main CCG organizations:

- Ship Safety Branch (DCGS): The Ship Safety Branch has the responsibility for developing and applying safety standards for all aspects of marine operation. This includes design, construction, operation, equipment, navigation, cargo and personnel standards. Also, as part of its overall responsibilities, this Branch drafts and amends the Small Vessel Regulations and Boating Restriction Regulations, tests and enforces small boat construction standards. It is also responsible for environmental protection and pollution prevention. In addition, a member of this branch acts as chairman of the Small Craft Committee of the Marine Safety Advisory Council (MSAC). Finally, the Branch provides technical advice on safety requirements to other government departments and agencies, other groups in DOT, to the marine industry (including IMCO) and provides expert witnesses at court hearings.

- Casualty Investigation (CCGI): This office is the custodian of the Marine Casualty Reporting System and is reponsible for performing casualty investigations and for recommending the development of proposals for new or revised legislation, regulations and directives in light of their findings. Casualty Investigation prepares and analyses statistical data on marine casualty trends and incidents, assesses their human, navigational or equipment problems and recommends remedial measures.

- Legislation Development (CCLM): This office is engaged in the preparation of the Maritime Code, which will eventually replace the Canada Shipping Act. It is responsible for the Arctic Waters Pollution Prevention Act, the Carriage of Goods by Water Act and the Government Vessels Discipline Act. Also, it develops policy alternatives for shipping legislation, represents the Department at interdepartmental meetings concerning proposals for new or amended legislation and prepares documents and assists in the submission of legislation to Parliamentary Committees.

- Search and Rescue (CGVR): The SAR division of Fleet Systems Branch has a headquarters superintendent position responsible for the Canadian Marine Rescue Auxiliary (CMRA) and Prevention, and an officer's position for Education and Prevention. Since 1977 this office has co-ordinated a SAR prevention program including the preparation of educational material such as pamphlets on boat equipment, films, media promotion and the Canadian Boating

Handbook, which has a distribution close to one million. This organization has also developed an extensive small craft courtesy inspection program.

In addition, the Marine Safety Advisory Council (MSAC) includes representation from all aspects of marine industry and, in particular, the Small Craft Committee chaired by the CCG which involves representatives from the Canadian Yachting Association, Canadian Power Squadrons, Allied Boating Association, Canadian Boating Federation, the Canadian Red Cross, Canada Safety Council, the Ontario Marine Operators Association, the Royal Lifesaving Society and other groups.

Research and Development activities are conducted and sponsored by these various groups although once again, the extent of specific safety objectives is not always clear. This is evident from a review of marine R&D projects for the year 1980*. While projects relating to e.g. ice management and navigational aids and traffic management are safety motivated to a large extent, the situation tends to be less clear-cut in areas such as vessels' and systems' technology.

A.8 Multimodal Transportation Safety - Transportation of Hazardous Materials

Concern for the safe transport of hazardous or dangerous materials has greatly increased in the minds of public decision-makers in all modes of transportation. In most countries, including the United States and Canada, hazardous materials transportation programs are an integral part of each mode's safety program and are not centralized within the administration. In the United States, a Task Force was established to investigate the adequacy and effectiveness of the various hazardous material programs in the areas of regulation, compliance, enforcement, training and emergency response, together with the organizational structure required to implement these programs*. At the present time, promulgation of hazardous materials regulations is centralized in the Research and Special Projects Administration (RSPA). Development of these regulations however, is conducted in the various operating administrations. Recommendations included establishment of a Standing Committee on Hazardous Materials, a National Hazardous Materials Response Centre (at USCG) and a centralized Hazardous Materials Information System.

In Canada, the Transportation of Dangerous Goods Directorate (TDG) of Transport Canada has a new act (Transportation of Dangerous Goods Act of 1980) permitting the regulation of dangerous goods transportation, but no regulations. Draft regulations have been published but have received a generally negative response from the carriers and industry. Part of the problem is that the new Code is based on the IMCO Code whereas the existing Red Book (which covers all land modes except trucking) is based on the U.S. "Title 49" code.

---

* Sandra Murphy-Wong, Listing of Canadian Marine R&D Projects 1980. Prepared for Transportation Development Centre at the request of Marine Transportation R&D Advisory Board, July 1981.

** United States, Department of Transportation, Hazardous Materials Task Force, Report of the Hazardous Materials Transportation Task Force. DOT Office of Management Planning, Office of the Secretary, September 1978.

The situation that will exist when the new Transport Canada regulations are promulgated is not clear. Sections of the Red Book (e.g., on tank car specifications) will still be in force. RTC would like to retain full control over inspection and compliance in the rail area. Transport Canada wants the provinces involved in inspection.

The Transportation of Dangerous Goods Directorate (TDG) has done considerable research in the areas of labelling/placarding systems, training packages and development of an Emergency Responsive Centre. TDG's effort has been aimed at both prevention and at reducing the consequences of accidents. In the prevention area, TDG is interested in methods of assessing the probabilities of an accident occurring. A uniform accident/incident reporting system is needed in this area.

Other multimodal issues are not particularly evident. The proposed establishment of an independent Accident Investigation Board for all modes (similar to the U.S. National Transportation Safety Board) is under consideration.

A.9 State of the Art of System Safety

A.9.1 Introduction

In discussing the state of the art of system safety, it is important to maintain the distinction between system safety as a management technique to implement safety objectives, and the application of system safety methods and techniques to identify areas of R&D need in safety. This section will concentrate more specifically on the first of these areas, the area for which the concept of system safety was originally conceived. Discussion of the second area, the area of particular interest to the present study, will be reserved for the next chapter.

This section is divided into the following parts:

- genealogy of the system safety approach;
- description of the system safety approach;
- safety measurement:
- preliminary evaluation.

A.9.2 Genealogy of the System Safety Approach

The concept and techniques of system safety analysis have existed for about 30 years. These techniques were originally conceived and have been used extensively and effectively by the U.S. Military, NASA and the aerospace industry. In fact, aircraft, particularly large commercial jet aircraft, are designed using a system safety analysis approach. More recently, the U.S. Atomic Energy Commission has applied these techniques.

The common denominator to the development of these applications appears to be:

- development of a system (including equipment and procedures) without historical precedent;

- complexity of the system;

- the catastrophic nature of the consequences of system failure (in terms of property or human loss);

- the high degree of management control that can be applied to the system as a whole.

In these cases, the need to identify, at the earliest stages of design, all possible elements or combinations of causes that might contribute to the failure of a system, led to the development of a set of formalized procedures for safety analysis, named system safety. In addition to this type of analysis, system safety also includes a set of managerial, contractual, manufacturing, testing and operational procedures to assist management in the decision-making process regarding hazard elimination and control.

A.9.3 Description of the System Safety Approach

While an extensive literature is available to describe and discuss the system safety approach, (cf. Bibliography, Appendix E) the most comprehensive and succinct description is provided by the U.S. Department of Defence in its "System Safety Program Requirements", (MIL-STD-882A, 1977). This is reproduced in its entirety in Appendix B.

Clearly, the description given in Appendix B is not oriented to transportation. In Appendix C, we reproduce a brief outline showing the adaptation of these planning procedures to transportation. Rather than reproduce that material here, we bring forward from both Appendices a set of definitions which are generally accepted among proponents of systems safety (cf. definitions in chapter 1).

- Safety. Freedom from those conditions that can cause death, injury, occupational illness, or damage to or loss of equipment or property.

- System. A composite, at any level of complexity, of operational and support equipment, personnel, hardware, and software procedures which are used together as an entity and capable of performing and/or supporting an operational role.

- System Safety. The tools, techniques and methodology used to obtain an optimum degree of safety within the constraints of operational effectiveness, time and cost. The goal is attained through specific application of system safety management and engineering principles throughout all phases of a system activity cycle.

- Accident (Mishap). An unplanned series of events that result in death, injury, occupational illness, or damage to or loss of equipment or property.

- Risk. An expression of a possible loss in terms of hazard severity and hazard probability.

- Hazard. An existing or potential condition that can result in an accident.

- Hazard Probability. The likelihood, expressed in quantitative or qualitative terms, that a hazard will occur.

- Hazard Severity. A qualitative assessment of the worst potential consequence, defined by the degree of injury, occupational illness, property damage, or equipment damage that could ultimately occur.

The heart of the analytical techniques of system safety is the identification and evaluation of hazards. A compendium of 25 such techniques is reproduced in Appendix D. From this list, the most well-known are the following:

- criticality analysis;
- event-tree analysis;
- failure modes and effects analysis;
- fault-tree analysis;
- single point failure analysis.

In each case, in Appendix D, a brief description is given, including method, application, difficulties, mastery required, comments and references.

A.9.4 Safety Measurement

Various measures of safety are used in the management of safety. Basically, the measure is the number of accidents per unit of exposure (denominator). The four major exposure bases are:

Base	Exposure Measure
Time	vehicle, passenger hours, system year
Event	# operations, number of takeoffs/landings, # entries/exits from harbour etc.
Activity	vehicle kilometers passenger kilometers
Population	# registered vehicles, # licenced drivers, # residential population, # drivers

A.9.5 Preliminary Evaluation of Systems Safety

Assessment of strengths (including success factors) and weaknesses of system safety cannot be made in isolation of its potential applications, i.e., in isolation of the user community. Three potential users/applications may be considered for purposes of the present study:

- military/aerospace system management;
- transportation system management;
- transportation safety R&D planning.

Only the first two users/applications are considered here.

System safety as a management/engineering approach to the achievement of safety (in the sense of "mission accomplishment") objectives in military or aerospace systems has evidently proved its mettle with such programs as the Apollo Moon Mission, the Minuteman Program and the Space Shuttle Project. Not only did such programs sponsor the development of the techniques involved, they also account for by far the largest volume of system safety work. The main success factors are two-fold:

- a self-contained and well defined system with clearly demarcated system boundaries and objectives;

- a high (if not exclusive) degree of management (including funding) control over the lifecycle of the system.

The management aspect is key, since traditionally, system safety developed as an engineering discipline, using design engineering methods and techniques. In the case of the U.S. Naval Air Systems Command for example, System Safety Management (SSM) is a major priority to the point that no program activities proceed until the System Safety Management Plan or SSMP is finalized. Only then does System Safety Engineering (SSE) begin.

Practitioners of system safety, however, typically find very different conditions when they seek to expand into other fields, in our case into the more general area of transportation safety. For example, in its first System Safety, State-of-the-Art conference held in Crystal City, Arlington, Virginia on November 4, 1981, the Washington D.C. Chapter of the System Safety Society concluded that "System Safety, although it is beginning to break out of the original military-aerospace beginnings, is not yet armed with techniques most needed for safety in commerce and in transportation safety"*. Participants agreed that there were seven basic constituent elements to a System Safety Program Plan (SSPP):

- defining the system;
- analysing the interfaces;
- complying with existing safety criteria;
- identifying new hazards;
- closing the loop to alleviate hazards;
- documenting management acceptance of risk;
- monitoring performance during system's service life.

Implementation of such plans, however, clearly requires a degree of management control which is largely absent in many areas of transportation. For example, in the case of the FAA, the attempt to apply system safety to teh general aviation system was hindered by the diversity and size of the "system". The road mode is perhaps the most extreme case of system fragmentation and consumer choice. For these reasons, road safety agencies do not define accident losses in terms of absent system organization, but in terms of the circumstances surrounding particular types of accident. A further difficulty is inherent in the dual orientation of system safety as system safety engineering (SSE) and system safety management (SSM). The traditional engineering approach to system design tends to relegate the human factor beyond the boundaries of the methodology. Finally, putting system safety to work in transportation (among other applications) is hampered by the difficulty of demonstrating a significant and immediate payoff. One observer pointed out that there is still no way to count accidents prevented by system safety analyses. Politically, however, such analyses are only acceptable if they are cost-beneficial. In times of funding contraints, the keynote is always proof-of-necessity. The corollary to this is that government sees safety as an additional branch in the management of the public's affairs; that is, safety can be emphasized as an independent subject, only if it appears that losses are large or prominent in the eyes of public opinion.

---

* Erskine E. Harton and Joseph T. Pizzo, "The State-of-the-Art of System Safety", Hazard Prevention, May/June 1982.

A.10 Conclusions

The most important result of the fact-finding stage of work on this project (task 1) may be summarized as follows:

- A distinction must be made between system safety as a management and engineering approach for the achievement of safety (or reliability) objectives of a technical system, and the application of system safety techniques to the identification of R&D needs in the field of safety (specifically of transportation safety).

- A variety of methods have been developed and applied to assist in establishing research and development needs.

- "System safety" techniques have been developed and applied to assist in establishing R&D needs in the area of safety enhancement programs.

- Use of system safety techniques and methodologies are more appropriate for the establishment and selection of programs and activities geared to accident prevention as opposed to accident protection or emergency response.

- No methods have been developed for universal application to all modes of transportation.

- No entirely defensible method has yet been devised that would unequivocally demonstrate the degree of safety improvement achievable through R&D and other system changes. This complicates the "proof- of-necessity" criterion.

- Difficulty has been experienced in implement ing methods designed to assist R&D needs establishment in government agencies (specifically in U.S. government transportation agencies).

The lessons to be learned from these results for future stages of work on this project are as follows:

- Attention should be given to R&D planning methods developed for U.S. and Canadian government agencies responsible of safety, in particular:

  - U.S. Coast Guard;
  - Urban Mass Transportation Administration;
  - Federal Highways Administration;
  - National Highway Traffic;
  - Safety Administration;
  - Federal Railroad Administration;
  - Canada Grains Council (not specifically safety related);
  - National Air Transportation Safety Plan (NATSP).

- Greater attention should be given to the institutional and political factors that govern the success or failure of implementing such a system.

With respect to this latter requirement, it must be remembered that the activities of government agencies are governed by a variety of mission objectives. Policies and programs will vary in the degree of attention devoted to safety. At one end of the spectrum, safety may be an exclusive or principle objective of the program. Alternatively, safety may be either a spin-off, or more likely, a constraint on program output. Furthermore, the beneficiaries of safety may be very different. It may be the Agency itself (i.e., safety of its own operations, or the operations it performs for the public) or it might be the public at large (e.g. regulatory programs). Costs and benefits may be very specific and easily identified, or they may be widely diversified and amorphous. Proof-of-necessity of research and development designed in support of these various types of programs and program objectives, must necessarily be based in part on such considerations, as well as on the institutional structures that exist (or are created) to implement a particular methodology in a given political and institutional context.

Finally, the problem of establishing R&D needs in the transportation safety area cannot be separated from the overall problem of establishing acceptable levels of risk in transportation. This is ultimately a matter of social (and therefore also political) values and no methodology is yet available to evaluate the perceived benefits of decreasing public exposure to risk. A curious ambivalence or "double standard" regarding safety in our society has been noted*. While there is increasing concern for the "safety" of new technologies in the field of nuclear emergy generation for example, there is a corresponding apathy or even resistance in applying correspondingly high safety standards to activities on the roads or at home where the number of fatalities and injuries is thousands of times greater. How much safety is safe enough must thus always remain a "grey area" for decision-makers.

---

* cf. Ludwig Benner Jr. "Safety, Risk and Regulation: Basic Concepts for Safety Risk Analysis". Transportation Research Forum Proceedings, 1973.

APPENDIX B

U.S. DEPARTMENT OF DEFENSE REQUIREMENTS FOR A SYSTEM SAFETY PROGRAM

(MIL-STD-882A, 1977

SYSTEM SAFETY MANAGEMENT

The New DOD Program Requirements (The "A" Revision to MIL-STD-882)

The substance of the new military standard on "System Safety Program Requirements" is reproduced for the benefit of those system safety managers, whether or not involved in military procurement efforts, who wish to know about these minimal criteria for an effective system safety engineering effort.

Foreword

The principal objective of a system safety program within the Department of Defense is to ensure that safety, consistent with mission requirements, is designed into systems, subsystems, equipment, and facilities, hereinafter referred to as systems.

DOD has approved this military standard for all DOD departments and agencies to use in developing system safety programs.

The degree of safety achieved in a system depends directly on management emphasis. Government and contractors will apply management emphasis to safety during the system acquisition process and throughout the life cycle of each system.

The success of the system safety effort depends on definitive statements for safety objectives and requirements by the managing activity and their translation into functional hardware. A formal safety program that stresses early hazard identification and elimination or control is the principal contribution of effective system safety. Selective application and the tailoring of this military standard shall be accomplished, as indicated herein, to specify the extent of contractual and DOD in-house compliance.

1. Scope

1.1 PURPOSE. This standard provides uniform requirements for developing and implementing a system safety program of sufficient comprehensiveness to identify the hazards of a system and to ensure that adequate measures are taken to eliminate or control the hazards.

1.2 APPLICATION. This standard applies to DoD systems and facilities, including support, test, maintenance, and training equipment. It applies to all phases of the system life cycle; e.g., design, research and development, test and evaluation, production, operation and support, and modification and disposal. The requirements shall also be applied to DoD in-house programs.

1.3 IMPLEMENTATION.

1.3.1 System safety program. A system safety program shall be developed according to the requirements of this standard. The requirements for a system safety program shall be included in all applicable contracts negotiated by the DoD managing activities. These contracts include those negotiated (a) within each DoD agency, (b) by one DoD agency for another, and (c) by DoD for other government agencies. In addition, a system safety program will be developed for each DoD in-house program.

1.3.2 System safety program plan. System safety program planning shall be included in all phases of DoD system acquisition documentation. For major systems acquisition or planned acquisition, a system safety program plan shall be developed. For nonmajor programs, system safety program plans shall be developed based on criteria such as mishap risk or as specified by the managing activity. The managing activity will either develop the system safety program plan or the contractor shall develop the plan based on system safety program requirements established by the managing activity. System safety program plans shall describe in detail how the program will be organized and conducted to implement the requirements of sections 4 and 5 of this military standard.

1.3.3 Contractual requirements. Tailored system safety program requirements shall be specified in the contractual provisions to include input to the statement of work, contractor data requirements list (CDRL), general and special provision sections, annexes, and other contractual means. When a system safety program plan is required, the plan shall be submitted with the contractor's proposal and be subject to contract negotiation. Upon approval by the managing activity, the system safety program plan shall be an attachment to the contract, referenced in the statement of work, and become the basis for contractual requirements. Format and content requirements for a system safety program plan are included in the Appendix.

1.3.4 Applicability. Each provision of this standard shall be reviewed by the managing activity to determine extent of applicability. Tailoring may take the form of deletion, alteration, or addition to the statements in 3, 4, and 5 to adapt this standard to specific system characteristics, program management options, contractual structure or life cycle phases (see 4.2). In tailoring the tasks, the detail and depth of the effort shall be defined by the managing activity and incorporated in the appropriate contractual or other program documents.

1.3.5 Duplication of effort. The managing activity shall review the contract for duplication of effort between system safety program requirements and other elements of the program (e.g., reliability, maintainability, and human factors). This review may also be required of a contractor. System safety program requirements and tasks shall be cross-referenced in the system safety program plan or other contract documentation to avoid duplication of effort by the managing activity and the contractor.

1.3.6 Conflicting requirements. The managing activity shall specify in the statement of work that when conflicting requirements or deficiencies are identified within system safety program requirements, the contractor shall submit notification, with supporting rationale and proposed alternatives, to the managing activity for resolution.

2. Referenced Documents

Referenced documents are not included in this document. Referenced documents required to supplement this military standard shall be specified in system specifications and contractual documents.

3. Definitions

The following definitions apply to this standard.

3.1 CONTRACTOR. A private sector enterprise or the organizational element of DoD (as used in this standard) engaged to provide services or products within agreed limits specified by the managing activity.

3.2 MANAGING ACTIVITY. The DoD organizational element of DoD that will plan, organize, direct, contract, and control tasks and associated functions appropriate to the life cycle phase of the system.

3.3 MISHAP. An unplanned event or series of events that result in death, injury, occupational illness, or damage to or loss of equipment or property.

3.4 RISK. An expression of possible loss in terms of hazard severity and hazard probability.

3.4.1 Hazard. An existing or potential condition that can result in a mishap (e.g., the presence of fuel in an undesired location is a hazard whereas the fuel itself is not).

3.4.2 Hazard probability. The likelihood, expressed in quantitative or qualitative terms, that a hazard will occur.

3.4.3 Hazard severity. A qualitative assessment of the worst potential consequence, defined by the degree of injury, occupational illness, property damage, or equipment damage that could ultimately occur.

3.5 SAFETY. Freedom from those conditions that can cause death, injury, occupational illness, or damage to or loss of equipment or property.

3.6 SYSTEM. A composite, at any level of complexity, of personnel, materials, tools, equipment, facilities, and software. The elements of this composite entity are used together in the intended operational or support environment to perform a given task or achieve a specific production, support, or mission requirement.

3.6.1 Subsystem. An element of a system that, in itself, may constitute a system.

3.7 SYSTEM SAFETY. The optimum degree of safety within the constraints of operational effectiveness, time, and cost attained through specific application of system safety management and engineering principles whereby hazards are identified and risk minimized throughout all phases of the system life cycle.

3.8 SYSTEM SAFETY ENGINEERING. An element of system engineering requiring specialized professional knowledge and skills in applying scientific and engineering principles, criteria, and techniques to identify, eliminate, or control system hazards.

3.9 SYSTEM SAFETY GROUP. A formally chartered group of persons organized to assist the program manager in achieving the system safety objectives.

3.10 SYSTEM SAFETY MANAGEMENT. An element of management that establishes the system safety program requirements and ensures the planning, implementation and accomplishment of tasks and activities to achieve system safety consistent with the overall program requirements.

3.11 SYSTEM SAFETY PROGRAM. The combined tasks and activities of system safety management and system safety engineering that enhance operational effectiveness by satisfying the system safety requirements in a timely, cost-effective manner throughout all phases of a system life cycle.

3.12 SYSTEM SAFETY PROGRAM PLAN (SSPP). A formal document that fully describes the planned safety tasks required to meet the system safety requirements, including organizational responsibilities, methods of accomplishment, milestones, depth of effort, and integration with other program engineering and management activities and related systems.

4. General Requirements

4.1 SYSTEM SAFETY PROGRAM OBJECTIVES. The system safety program shall define a systematic approach to ensure that:

a. Safety consistent with mission requirements is designed into the system in a timely, cost-effective manner.

b. Hazards associated with each system are identified and evaluated, and eliminated or controlled to an acceptable level throughout the entire life cycle of a system.

c. Historical safety data generated by other systems are considered and used, where appropriate.

d. Minimum risk is involved in accepting and using of new designs, materials, and production and testing techniques.

e. Retrofit actions required to improve safety are minimized through the timely inclusion of safety features during development and acquisition of a system.

f. Modifications do not degrade the inherent safety of the system.

g. Consideration is given to safety and ease of disposal and demilitarization of any hazardous materials associated with the system.

4.2 SYSTEM SAFETY PROGRAM REQUIREMENTS RELATED TO LIFE CYCLE PHASES. The system safety program requirements are related here to the life cycle of a major system to show how the requirements of this military standard will be met. When the system program is not designated as a major program, the phases will be related to the major system life cycle phases to determine the safety tasks required. The system safety program requirements relating to each life cycle phase shall be selectively applied and tailored depending on the intended use of the system. If the acquisition has been in process before establishing the requirement for a system safety program, system safety program requirements normally performed during earlier phases will be evaluated for applicability to ensure risk is minimized. In all cases, the system safety program should be developed to facilitate continuation of the system safety effort into subsequent phases of the life cycle sequence; i.e., program initiation, demonstration and validation, full-scale engineering development, and production and deployment (including operation, support, and disposal).

4.2.1 Milestone 0 – program initiation

4.2.1.1 Milestone 0. The system safety effort will support the definition of mission element needs by identifying safety deficiencies in existing or projected capability and by identifying opportunities for system safety to improve mission capability or reduce life cycle costs.

4.2.1.2 Program initiation phase. System safety tasks applicable to the program initiation phase are those required to evaluate the alternative system concepts under consideration for development and establish the system safety program consistent with the identified mission need and life cycle requirements. System safety tasks will include the following:

a. Evaluate all material, design features, procedures and operational concepts and environments under consideration which will affect safety throughout the life cycle.

b. Perform a preliminary hazard analysis (PHA) to identify hazards associated with each alternative concept.

c. Identify possible safety interface problems.

d. Highlight special areas of safety consideration, such as system limitations, risks, and man-rating requirements.

e. Review safe and successful designs of similar systems for consideration in alternative concepts.

f. Define the system safety requirements based on past experience with similar systems.

g. Identify safety requirements that may require waiver during the system life cycle.

h. Identify any safety design analysis, test, demonstration and validation requirements.

i. Document the system safety analyses, results, and recommendations for each promising alternative system concept.

j. Prepare a summary report of the results of the system safety tasks conducted during the program initiation phase to support the decision-making process.

k. Tailor the system safety program for the subsequent phases of the life cycle and include detailed requirements in the appropriate demonstration and validation phase contractual documents.

4.2.2 Demonstration and validation phase. System safety tasks during the demonstration and validation phase will be tailored to programs ranging from extensive study and analyses through hardware development to prototype testing, demonstration and validation. System safety tasks will include the following:

a. Prepare or update the SSPP to describe the proposed integrated system safety effort planned for the demonstration and validation phase.

b. Perform or update the PHA performed during the program initiation phase. Prepare a PHA report of the proposed system concept in its intended use and operational environment.

c. Identify those technology, design, production, and operational and support (O&S) risks having an impact on safety.

d. Establish system safety requirements and criteria for verifying that requirements have been met.

e. Participate in trade-off studies to reflect the impact on system safety requirements and risk. Recommend system design changes based on these studies to ensure that the optimum degree of safety is achieved consistent with performance and system requirements.

f. Identify for inclusion in the appropriate specifications any qualitative and quantitative system safety requirements for the system. Include contractor-furnished equipment, government-furnished equipment, ground support equipment, and all interfacing and ancillary equipment.

g. Perform subsystem, system, and operating and support (O&S) hazards analyses.

h. Review all test plans to ensure safe conduct of the tests.

i. Ensure that hazards identified by analyses and tests are eliminated or controlled.

j. Review training plans and programs for adequate safety considerations.

k. Evaluate results of failure analyses and mishap investigations recorded during the demonstration and validation phase. Recommend redesign and other corrective action.

l. Ensure that system safety requirements are incorporated into the system specification based on updated system safety studies, analyses, and tests.

m. Prepare a summary report of the results of the system safety tasks conducted during the demonstration and validation phase to support the decision-making process.

n. Continue to tailor the system safety program. Prepare an SSPP for the full-scale engineering development phase and initial production phase.

4.2.3 Full-scale engineering development phase. To provide support to the system engineering program, the system safety tasks during the full-scale engineering development phase will include the following:

a. Ensure effective and timely implementation of the SSPP for the full-scale engineering development phase.

b. Review preliminary engineering designs to ensure that safety design requirements are incorporated and hazards identified during the demonstration and validation phase are eliminated or controlled.

c. Update system safety requirements in system specifications.

d. Perform or update subsystem, system, and O&S hazard analyses and safety studies concurrent with the design/test effort to identify design and operating and support hazards. Recommend any required design changes and control procedures.

e. Identify testing facilities, test requirements, specifications, and criteria to ensure that design safety is verified. Review the test plans and programs to ensure safe conduct of the tests.

f. Participate in technical design and program reviews and present results of subsystem, system, and O&S hazard analyses.

g. Identify and evaluate the effects of storage, shelf-life, packaging, transportation, handling, test, operation, and maintenance on the safety of the system and its components.

h. Evaluate results of failure analyses and mishap investigations recorded during full-scale engineering development. Recommend redesign or other corrective action.

i. Identify, evaluate, and provide safety considerations for trade-off studies.

j. Review appropriate engineering documentation (drawings, specifications, etc.) to ensure safety considerations have been incorporated.

k. Review, and provide safety inputs to, preliminary system operation and maintenance publications.

l. Verify the adequacy of safety and warning devices, life support equipment, and personal protective equipment.

m. Provide safety inputs to training courses.

n. Review the preliminary production engineering effort including purchase specifications, process quality control, inspection and acceptance, and test procedures to ensure that safety in the process and end product is established and maintained during production.

o. Ensure requirements are developed for demilitarization and for safe disposal of hazardous materials and equipment.

p. Prepare a summary report of the results of the system safety tasks conducted during the full-scale engineering development phase to support the decision-making process.

q. Tailor system safety program requirements for the production and deployment phase.

4.2.4 Production and deployment phase. As part of the on-going system safety program, the system safety tasks during the production and deployment phase will include the following:

a. Prepare or update the SSPP to reflect the system safety program requirements for the production and deployment phase.

b. Identify critical parts and assemblies, production techniques, assembly procedures, facilities, testing, and inspection requirements which may affect safety and will ensure:

(1) Adequate safety provisions are included in the planning and layout of the production line to establish safety control of the system within the production process and operations.

(2) Adequate safety provisions are included in inspections, tests, procedures, and checklists for quality control of the equipment being manufactured so that safety achieved in design is maintained during production.

(3) Production technical manuals or manufacturing procedures contain required warnings, cautions, and special procedures.

c. Verify that testing and evaluation is performed on early production hardware to detect and correct safety deficiencies at the earliest opportunity.

d. Review test plans and programs to ensure safe conduct of the tests.

e. Review warnings, cautions, and special procedures required for safe operation and maintenance.

f. Review procedures for storage, packaging, handling, and transportation to ensure that safety is maintained.

g. Review procedures and monitor results of periodic field inspections or tests (including recall-for-tests) to ensure acceptable levels of safety are maintained. This includes identifying major or critical characteristics of safety significant items that deteriorate with age, environmental conditions, or other factors.

h. Update hazard analyses to identify any new hazards that may result from engineering changes. Ensure that the safety implications of the changes are considered in all configuration control actions.

i. Evaluate results of failure analyses and mishap investigations. Recommend corrective action.

j. Monitor the system throughout the life cycle to determine the adequacy of the design, and operating, maintenance, and emergency procedures.

k. Conduct a safety review of proposed new operating and maintenance procedures, or changes, to ensure that the procedures, warnings, and cautions are adequate and inherent safety is not degraded. These reviews shall be documented as updates to the O&S hazards analyses.

l. Analyze safety deficiency reports submitted by operating and support personnel.

m. Review capability and procedures for demilitarization and disposal of hazardous material and equipment.

n. Document hazardous conditions and system deficiencies for development of follow-on requirements for modified or new systems.

o. Update safety documentation, such as design handbooks, military standards and specifications, to reflect safety "lessons learned".

5. Detailed Requirements

5.1 DEVELOPMENT OF THE SYSTEM SAFETY PROGRAM. A total program shall be developed in which design analyses, studies, and testing will identify system performance limitations, failure modes, safety margins, and critical operator tasks. All known facets of safety optimization including design, engineering, education, management policy and supervisory control shall be considered in the identifying and eliminating or controlling hazards. System safety management and engineering shall be integrated with other management and engineering disciplines in the interest of an optimum system design. Procedures for development and integration of the system safety effort shall be applied across the managing activity/contractor interface to assure a system safety program consistent with overall system requirements.

5.1.1 Managing activity responsibilities. The managing activity shall:

a. Establish, plan, organize, and implement an effective system safety program that is integrated into all life cycle phases.

b. Establish definitive system safety program requirements for the procurement or development of a system. The requirements shall be set forth clearly in the appropriate system specifications and contractual documents and define:

(1) In the appropriate system specifications, the system safety performance and design requirements that are available and applicable.

(2) In the statement of work, the system safety requirements that cannot be defined in the system specifications. This would include general design guidelines in 5.4.1.

(3) In the statement of work and CDRL as applicable, the specified safety data; e.g., analyses, tests, or progress reports that will be required during the scope of the effort.

c. Ensure that an SSPP is prepared that reflects in detail how the total program is to be conducted.

d. Review and approve for implementation the SSPPs prepared by the contractor.

e. Supply historical safety data as available.

f. Monitor contractors' system safety activities and review and approve deliverable data, if applicable, to ensure adequate performance and compliance with system safety requirements.

g. Ensure that the appropriate system specifications are updated to reflect results of analyses, tests, and evaluations.

h. Evaluate new design criteria for inclusion into military specifications and standards and submit recommendations to the respective responsible organization.

i. Establish system safety groups as appropriate to assist the program manager in developing and implementing a system safety program.

5.1.2 Contractor responsibilities. The contractor shall:

a. Develop and submit an SSPP describing the proposed integrated safety effort in response to the specific requirements at the managing activity.

b. Establish a system safety organization or function that shall manage and perform the overall system safety program.

c. Ensure effective and timely implementation of the SSPP, approved by the managing activity, and the system safety program in accordance with the contractual requirements.

d. Establish interfacing procedures to subcontractors to meet the requirements of the managing activity.

e. Support system safety group activities as required by the managing activity and according to the contractual requirements.

5.2 SYSTEM SAFETY ORGANIZATION. A system safety organization shall be provided for the conduct and management of the system safety program for both the managing activity and contractor. The responsibilities and functions of those directly associated with system safety policies and implementation of the program shall be clearly defined. The authority delegated to this organization and the relationship between line, staff, and interdepartmental, project, functional, and general management organization shall be identified. Personnel assigned to the system safety program shall be identified including their qualifications, specific experience, and formal education or training.

5.3 SYSTEM SAFETY PROGRAM MILESTONES AND REVIEWS. Each system safety program shall be planned to provide for periodic status reviews, presentations of hazard analyses and risk assessments, and evaluation of the overall effectiveness of the system safety effort. These reviews and assessments, conducted jointly by the managing activity and contractor, shall be performed concurrently with the appropriate program milestones. System safety shall be an agenda item of the appropriate scheduled program or design review held for the system to assess the status of compliance with the system safety requirements. These reviews shall identify any deficiencies of the system with respect to safety and provide guidance for further development. At the discretion of the managing activity, a system safety group may be established for selected systems or additional ad hoc safety reviews may be scheduled as required.

5.4 SYSTEM SAFETY REQUIREMENTS. System safety requirements establish design and operational safety criteria for hazard elimination or control and may establish a quantitative value designating the level of system safety.

5.4.1 General requirements. System designs and operational procedures should consider the following:

a. Review pertinent standards, specifications, regulations, design handbooks, and other sources of design guidance for applicability to the design of the system.

b. Eliminate or control hazards identified by analyses or related engineering efforts through design solution, material selection, or substitution. Potentially hazardous materials (e.g., propellants, explosives, hydraulic fluids, solvents, lubricants or fuels) shall be selected to provide optimum safety characteristics.

c. Isolate hazardous substances, components, and operations from other activities, areas, personnel, and incompatible materials.

d. Locate equipment so that access during operations, maintenance, repair, or adjustment minimizes personnel exposure to hazards (e.g., hazardous chemicals, high voltage, electromagnetic radiation, cutting edges, or sharp points).

e. Minimize hazards resulting from excessive environmental conditions (e.g., temperature, pressure, noise, toxicity, acceleration and vibration).

f. Design to minimize human error in the operation and support of the system.

g. Consider alternate approaches to minimize hazards that cannot be eliminated. Such approaches include interlocks, redundancy, fail-safe design, system protection, fire suppression, and protective clothing, equipment, and devices.

h. Protect the power sources, controls and critical components for redundant subsystems by physical separation or shielding.

i. Provide suitable warning and caution notes in assembly, operations, maintenance, and repair instructions, and distinctive markings on hazardous components, equipment, or facilities to ensure personnel and equipment protection. These shall be standardized in accordance with the requirements of the managing activity.

j. Minimize the severity of personnel injury or damage to equipment in the event of a mishap (e.g., by incorporating crashworthy design features in all man-rated systems).

k. Review design criteria for inadequate or overly restrictive requirements regarding safety. Recommendations should be made for new design criteria supported by study, analyses, or test data.

5.4.2 System safety precedence. The order of precedence for satisfying system safety requirements and resolving identified hazards shall be as specified:

a. Design for minimum hazard. From the first, design to eliminate hazards. If an identified hazard cannot be eliminated, control hazards through design selection.

b. Safety devices. Hazards that cannot be eliminated or controlled through design selection shall be controlled to an acceptable level through the use of fixed, automatic, or other protective safety design features or devices. Provisions shall be made for periodic functional checks of safety devices.

c. Warning devices. When neither design nor safety devices can effectively eliminate or control an identified hazard, devices shall be used to detect the condition and to generate an adequate warning signal to correct the hazard or provide for personnel evacuation. Warning signals and their application shall be designed to minimize the probability of incorrect personnel reaction to the signals and shall be standardized within like types of systems.

d. Procedures and training. Where it is impossible to eliminate or adequately control a hazard through design selection or use of safety and warning devices, procedures and training shall be used to control the hazard. Procedures may include the use of personal protective equipment. Precautionary notations shall be standardized as specified by the managing activity. Safety critical tasks and activities may require certification of personnel proficiency.

5.4.3 Risk assessment. A risk assessment procedure commensurate with the system safety requirements shall be developed to establish priorities for corrective action and resolution of identified hazards. Since the priority for system safety is eliminating hazards by design, a risk assessment procedure considering hazard severity only will generally suffice during the early design phase to minimize hazards. When hazards are not eliminated during early design, a risk assessment procedure based upon the hazard probability, as well as hazard severity, may be required to establish priorities for corrective action and resolution of identified hazards. An example of a risk assessment is a numeric rank ordering of a mathematical combination arrived at by assigning numerical values to severity category and probability level.

5.4.3.1 Hazard Severity. Hazard severity categories are defined to provide a qualitative measure of the worst potential consequences resulting from personnel error, environmental conditions, design inadequacies, procedural deficiencies, system, subsystem or component failure or malfunction as follows:

Example of a qualitative hazard probability ranking

Descriptive Word	Level	Specific Individual Item	Fleet or Inventory
Frequent	A	Likely to occur frequently	Continuously experienced
Reasonably Probable	B	Will occur several times in life of an item	Will occur frequently
Occasional	C	Likely to occur sometime in life of an item	Will occur several times
Remote	D	So unlikely, it can be assumed that this hazard will not be experienced	Unlikely to occur but possible
Extremely Improbable	E	Probability of occurrence cannot be distinguished from zero	So unlikely, it can be assumed that this hazard will not be experienced
Impossible	F	Physically impossible to occur	Physically impossible to occur

a. Category I - Catastrophic. May cause death or system loss.

b. Category II – Critical. May cause severe injury, severe occupational illness, or major system damage.

c. Category III - Marginal. May cause minor injury, minor occupational illness, or minor system damage.

d. Category IV - Negligible. Will not result in injury, occupational illness, or system damage.

These hazard severity categories provide guidance to a wide variety of programs. However, adaptation to a particular program may be required. This adaptation may include definite transition points between categories and further definition of the degree of injury or damage.

5.4.3.2 Hazard probability. The probability that a hazard will occur during the planned life expectancy of the system can be described in potential occurrences per unit of time, events, population, items, or activity. Assigning a quantitative hazard probability to a potential design or procedural hazard is generally not possible early in the design process. A qualitative hazard probability may be derived from research, analysis, and evaluation of historical safety data from similar systems. Supporting rationale for assigning a hazard probability shall be documented in hazard analysis reports.

5.4.4 Action on identified hazard. Action shall be taken to eliminate or minimize hazards revealed by analyses or related engineering efforts. Catastrophic and critical hazards shall be eliminated or controlled. If these hazards cannot be eliminated or controlled to an acceptable level, the alternative controls and recommendations will be immediately presented to the managing activity. Hazard analyses and reports shall provide closed-loop procedures to ensure timely resolution of all identified hazards.

5.5 HAZARD ANALYSES. Analyses are performed to identify hazardous conditions to effect their elimination or control during all life cycle phases. Analyses shall be made to systematically examine the system, subsystem, facility, components, software, personnel, and their interrelationship including logistics, training, maintenance, test, modification, and operational environments. The analyses shall be accomplished to do the following:

a. Identify hazards, determine any needed corrective actions, and establish corrective action priorities.

b. Determine and evaluate safety considerations in trade-off studies.

c. Determine and evaluate appropriate safety design and procedural requirements.

d. Provide documented evidence of compliance with specified safety tasks, objectives, and design requirements.

e. Support life-cycle-cost and design-to-cost analyses.

The selection of specific methods and techniques for performing these analyses is based on the level of complexity of the system element under consideration and the extent of system development. The hazard analyses methods and techniques selected for the system safety program should provide for continuity throughout the system life cycle and interfacing of results from one analysis to another to ensure identified hazards are corrected.

5.5.1 Analysis type, format and technique. Hazards analyses used in system safety are (a) preliminary hazards analysis (PHA) which is an initial safety assessment of the system, (b) subsystem hazard analysis (SSHA) which provides for hazard identification associated with the functional relationship of components and equipments comprising each subsystem, (c) system hazard analysis (SHA) which provides for hazard identification associated with subsystem interfaces, and (d) operating and support (O&S) hazard analyses which provide for an evaluation of procedural safety. Analyses may be qualitative or quantitative. The managing activity may specify the format and technique to be used for hazard analyses requiring submittal or integration. The format may be a structured or unstructured narration, a matrix chart, or a logic model. Models and techniques should be compatible with those being applied by other disciplines on the same program so that results are comparable.

5.5.1.1 Preliminary hazard analysis. A preliminary hazard analysis (PHA) shall be performed to obtain an initial risk assessment of a concept or system. The purpose of a PHA is to identify safety critical areas, evaluate hazards, and identify the safety design criteria to be used. The PHA effort shall be initiated during the program initiation phase or earliest life cycle phases of the program so that safety considerations are included in trade-off studies and design alternatives. Based on the best available data, hazardous conditions associated with the proposed design or function should be evaluated for hazard severity, hazard probability, risk, and operational constraint. Safety provisions and alternatives needed to eliminate or control hazardous conditions should be considered. The information shall be used in the developing system safety requirements and in preparing performance and design specifications. Also, the PHA is the basic hazard analysis which establishes the framework for other hazard analyses and safety engineering evaluation of the design. The PHA should consider the following for identification of hazards:

a. Hazardous components (e.g., energy sources, fuels, propellants, explosives, and pressure systems).

b. Safety related interface considerations among various elements of the system (e.g., material compatibilities, electromagnetic interference and other possibilities of inadvertent activation, fire/explosive initiation and propagation).

c. Environmental constraints including the normal operating environments (e.g., drop, shock, extreme temperatures, noise and health hazards, fire, electrostatic discharge, lightning, X-ray, electromagnetic radiation, and laser radiation).

d. Operating, test, maintenance and emergency procedures (e.g., human error analysis of operator functions, tasks, and requirements; effect of environmental factors such as equipment layout and lighting requirements on human performance; life support requirements and their safety implications in manned systems; crash safety; egress, rescue, survival, and salvage).

e. Facilities, support equipment, and training (e.g., provisions for storage, assembly, checkout, prooftesting of hazardous systems/assemblies which may include toxic, flammable, explosive, corrosive or cryogenic fluids; electrical power sources; training and certification pertaining to safe operation and maintenance).

f. Safety related equipment, safeguards, and possible alternate approaches (e.g., interlocks, system redundancy, failsafe design considerations, subsystem protection, fire suppression systems, and personal protective equipment).

5.5.1.2 Subsystem hazard analysis. An analysis applied to some element of the total system is called a subsystem hazard analysis (SSHA). SSHA shall be performed to identify hazards associated with component failure modes and functional relationships of components and equipments comprising each subsystem. Such analysis should identify all components and equipments whose performance, performance degradation, functional failure, or inadvertent functioning could result in a hazard. The analysis should include a determination of the modes of failure including all single point failures and the effects on safety when failures occur in subsystem components. SSHA should normally be performed during the demonstration and validation phase and should be started as soon as the actual design of the subsystem has been refined to the point where detailed design information is available. The format for this analysis must be carefully established to minimize problems in integrating subsystem hazard analyses into the system hazard analysis. Techniques that may be used to complete the SSHA include:

a. Fault hazard analysis – An inductive method of analysis which can be used exclusively as a qualitative analysis, or, if desired, expanded to a quantitative one. The fault hazard analysis requires a detailed investigation of the subsystem to determine component hazard modes, causes of those hazards, and resultant effects to the subsystem and its operation.

b. Fault tree analysis – A deductive analytical tool used to analyze all events, faults, and occurrences and all their combinations that could cause or contribute to the occurrence of a defined undesired event. A qualitative or quantitative analysis may be conducted.

c. Sneak circuit analysis – Conducted on hardware and software to identify latent (sneak) circuits and conditions that inhibit desired functions or cause undesired functions to occur, without a component having failed. The analysis employs recognition of topological patterns which are characteristic of all circuits and electrical/electronic systems.

5.5.1.3 System hazard analysis. System hazard analysis (SHA) shall be performed on subsystem interfaces to determine the safety problem areas of the total system. Techniques similar to those used for the SSHA should be used. Such analyses should include a review of subsystems interrelationships for:

a. Compliance with safety criteria.

b. Possible independent, dependent, and simultaneous failures that could present a hazardous condition including failures of safety devices.

c. Degradation in the safety of a subsystem or the total system from normal operation of another subsystem.

d. Changes that occur within subsystems so that the system hazard analysis can be updated accordingly.

5.5.1.4 Operating and support hazard analyses. Operating and support (O&S) hazard analyses shall be performed to identify and control hazards and determine safety requirements for personnel, procedures, and equipment used in production, installation, maintenance, testing, modification, transportation, storage, operation, emergency escape, egress, rescue, training, and disposal during all phases of intended use as specified in the system requirements. The O&S hazard analyses begun in the demonstration and validation phase should be oriented to development and operational testing. As the life cycle proceeds to production and deployment, O&S problems should be included. The analyses will also address hazards to the system that may be induced by maintenance personnel. Engineering data, procedures, and instructions developed from the engineering design and initial test programs should be used in support of this effort. Results of these analyses should provide the basis for:

a. Identifying a hazardous time period and actions required to minimize risk during this time.

b. Design changes to eliminate and control hazards.

c. Identifying requirements for safety devices and equipment and required maintenance procedures to detect their functional failure.

d. Warnings, cautions, and special and emergency procedures for operating and maintenance.

e. Special procedures for handling, storage, transportation, maintenance, and modification.

5.6 SYSTEM SAFETY DATA

5.6.1 Acquisition and use of Safety data. Safety data shall be used as an aid to prevent design deficiencies, particularly those of a repetitive nature. Safety data are accumulated from prior programs, similar systems, earlier work on an on-going program, and other historical sources. The data are used to evaluate the safety of a system, or verify compliance with the system safety requirements. These data shall include: (a) mishap reports, (b) mishap probabilities, (c) failure rates, (d) test results, (e) system safety analyses, (f) failure mode and effects analyses, and (g) human factors data. Liaison with other data sources shall be sought and maintained to identify hazards and evaluate safety design deficiencies.

5.6.2 Mishap reporting. The managing activity will specify requirements for reporting mishaps or malfunctions during the system safety program.

5.6.3 Deliverable data. The managing activity will specify the deliverable safety data requirements in the contractor data requirements list (DD Form 1423) attached to a request for proposal, invitation for bid, or the contract, as appropriate. The SSPP and other required system safety data and reports submitted by the contractor will be subject to review and approval by the managing activity as specified in the CDRL.

5.6.4 Nondeliverable data. Nondeliverable data shall be indexed, filed, and maintained by the contractor for the time specified by the managing activity. The data shall be made available at the contractor's facility for review and use by authorized representatives of the managing activity upon request.

5.7 SAFETY TESTING AND DEMONSTRATIONS. Tests and demonstrations shall be defined to validate selected safety features of the system. Tests or demonstrations shall be performed on safety critical equipment and procedures to determine the hazard severity or to establish the margin of safety of the design. Induced or simulated failures will be considered to demonstrate the failure mode and acceptability of safety critical equipment. Where hazards are identified during the development effort and it cannot be analytically determined whether the action taken will adequately control the hazard, safety tests shall be conducted to evaluate the effectiveness of the controls. Subsequent SSPPs and test program plans shall be revised to include these tests. Where costs for safety testing would be prohibitive, safety characteristics or procedures may be verified by engineering analyses, analogy, laboratory test, functional mockups, or subscale/model simulation, when approved by the managing activity. Specific safety tests shall be integrated into appropriate system test and demonstration plans to the maximum extent possible. Test plans, procedures, and test results for all tests including design verification, operational evaluation, production acceptance, and shelf-life validation shall be reviewed to ensure that:

a. Safety is adequately demonstrated.

b. The testing will be conducted in a safe manner.

c. All additional hazards introduced by testing procedures, instrumentation, test hardware, environment, etc., are properly identified and controlled.

5.8 TRAINING. Approved safety procedures shall be included in instruction lesson plans and student examinations for the training of engineering, technician, operating and maintenance personnel. Safety and warning devices, personal protective equipment, and emergency equipment shall be identified.

5.9 AUDIT PROGRAM. Techniques and procedures shall be implemented to ensure that the objectives and requirements of the system safety program are being accomplished. Procedures shall also be included for ensuring adequate on-the-job safety surveillance during system installation, checkout, maintenance, and modification activities.

5.10 OTHER SAFETY MATTERS. Specific requirements for other specialized safety activities (e.g., nuclear, range, explosive, chemical, biological, electromagnetic radiation, and lasers) shall be included as necessary to satisfy the requirements of the managing activity.

System Safety Program Plan

Format and content requirements for a system safety program plan shall be as specified by the managing activity and in accordance with one of the following data requirements: DD Form 1664 identification number – DI-R-3531 (USAF), DI-H-1320A (Army), UDI-H-20417 (Navy).

Editor's Note

MIL-STD-882A was issued, dated 28 June 1977, to supercede the widely used MIL-STD-882 that has been in effect for the past eight years. Copies of the new military standard will be available, starting in September, from the Naval Publications and Forms Center, 5801 Tabor Avenue, Philadelphia, Pa. 19120 (Customer Services Telephone 215-697-3321). Comments regarding the new standard should be made to Hq. Air Force Systems Command (IGFS), Andrews AFB, Washington, D.C. 20334. The new standard is approved for use by all Departments and Agencies of the U.S. Department of Defense. SSS member Joyce McDevitt has been involved in the development of this new military standard.

APPENDIX C

"SYSTEM SAFETY APPLICATIONS TO TRANSPORT SAFETY"

(PROCEEDINGS OF
THE FOURTH ANNUAL INTERSOCIETY CONFERENCE ON TRANSPORTATION
LOS ANGELES, 1976)

PROCEEDINGS

DOT-TSC
FEB 3 -76
LIBRARY
[illegible]

Fourth Annual Intersociety Conference on Transportation

July 18 - 23, 1976
Los Angeles, California

Member Societies

American Society of Mechanical Engineers
American Economic Association
American Institute of Aeronautics and Astronautics
American Institute of Industrial Engineers, Inc.
American Railway Engineering Association
American Society of Civil Engineers
Engineering Institute of Canada
Institute of Electrical and Electronics Engineers, Inc.
Institute of Management Sciences
Institute of Traffic Engineers
Operations Research Society of America
Society of Automotive Engineers
The Society of Naval Architects and Marine Engineers

TE-2

SYSTEM SAFETY APPLICATIONS TO TRANSPORTATION SAFETY[*]

N. Horodniceanu, Research Assoc., Dept. of Transportation Planning & Engineering
E. J. Cantilli, Assoc. Professor, Dept. of Transportation Planning & Engineering
M. Shooman, Professor, Dept. of Electrical Engineering
L.J. Pignataro, Professor & Head, Dept. of Transportation Planning & Engineering

Polytechnic Institute of New York.

ABSTRACT

This paper reviews existing system safety techniques and discusses their possible transfer and aplicability to transportation safety. An application of system safety analysis techniques to an automobile braking system is presented.

INTRODUCTION

Through the years, system analysis techniques have been devised and used to maximize system design and operating objectives. Their intent has been to enable decision makers to reach correct conclusions, using an orderly process of data collection, modeling, analysis management and evaluation.

As the system analysis discipline has developed distinct sub classes, such as control, communications, reliability, and safety analysis have appeared. Many of these disciplines, especially safety and reliability, have been encouraged in their development by DOD and NASA requirements.

The need to identify, at the earliest stages of design, all possible elements or combinations of causes that might contribute to a failure of the system, led to the development of a set of formalized procedures for safety analysis, named system safety. These procedures required a logical examination of all elements of a system and the identification of all possible sources of accidents. The analysis does not end with the identification of hazards, but estimates the probability of their occurrence, and points out available options for their elimination. In addition to safety analysis, system safety includes a set of managerial, contractual, manufacturing, testing and operational procedures. This has proved to be an invaluable managerial tool in improving the decision-making process regarding hazard elimination, hazard control, and risk taking.

System safety analysis is a relatively new discipline, and its techniques have been used effectively by the military, the aerospace industry, and, more recently, by the atomic energy commission on projects where designs, equipment, and procedures were developed without precedents(for guidance), and where the consequences of failure are extremely serious.

For better understanding, the terms "Safety", "System", and "System Safety", must be clarified and defined.

- Safety - freedom from those conditions that can cause injury or death to personnel, or damage to or loss of equipment or property.
- System - a composite, at any level of complexity, of operational and support equipment, personnel, hardware, and software and procedures which are used together as an entity and capable of performing and/or supporting an operational role.
- System Safety- the tools, techniques, and methodology used to obtain an optimum degree of safety within the constraints of operational effectiveness, time and cost. The goal is attained through specific application of system safety management and engineering principles throughout all phases of a system activity cycle.

A transportation system's activity cycle includes all phases from concept formulation through operation. Since not all systems follow these phases as distinctly as stated, each system safety program plan and activity must be adapted to the specific requirements of the system or project.

SYSTEM SAFETY PROGRAM

The system safety program objectives described in MIL-STD-882, (System Safety Program for Systems and Associated Sub-Systems and Equipment, July 1969) are intended to insure that:

- Safety, compatible with the system's requirements, is incorporated at the design stage.
- Hazards associated with each system are identified, and either eliminated, or minimized, so as to obtain an acceptable level of safety.
- The acceptance and use of new materials, new production methods and new testing techniques involves a minimal risk.
- Safety improvements required after the construction and operation of a system will be minimized.
- Historical safety data generated by similar systems is analyzed and used where appropriate.

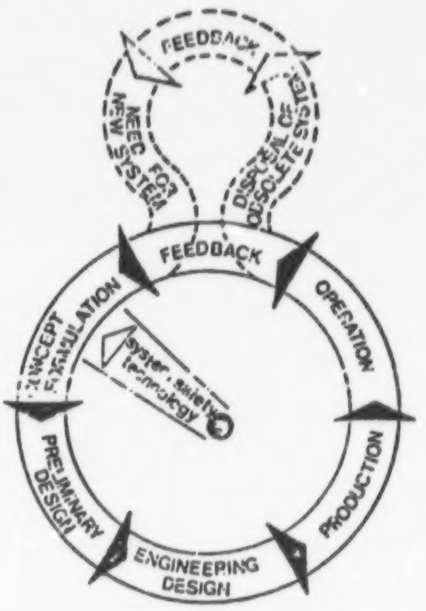
Such a program is developed based upon the system objectives, criticality of the safety requirements, complexity of design, and total cost. Obviously, the objectives stated above are applicable to systems outside the military, although special adaptation, interpretation, and ordering of priorities, may be required.

Regardless of the performing agency, it is clear that a safety program will have to employ and combine both managerial and analytical techniques. A project, particularly a new one, can be divided into several distinct parts, based on its evolutionary development. There are five distinct levels attached to such a transportation activity system cycle: (see Figure 1)

- Conceptual Level
- Contractual and Preliminary Design Level
- Engineering Design Level
- Production Level
- Operational and Maintenance Level

---

[*] This document was prepared under the sponsorship of the United States Department of Transportation in the interest of information exchange. The United States Government assumes no liability for its contents or use thereof.



TRANSPORTATION ACTIVITY CYCLE (TAC) RING

FIGURE 1

The origin of this cyclic ring is with the military. The Department of Defense standards refer to it as a "system life cycle", and carry it until "disposal". In adapting this "life cycle" approach to transportation, we must realize that "disposal" of a system, such as a rail network or a highway facility, is often not a valid assumption. It is more conceivable that the cyclic ring will be followed from conception through operation, with feedback to the con-conceptual phase, based on operating knowledge, for the purposes of improving existing systems and building new ones.

Any safety program should follow the phases described above. The primary function of such a program is to assist management in its attempt to achieve the basic safety goals and objectives of the system. The preparation of a System Safety Program Plan (SSPP) is the backbone of a systematic approach to the problem. The development of such a plan is usually divided into two basic phases:

- Preparation of a preliminary SSPP
- Preparation of a final SSPP

The preliminary system safety program phase is primarily a managerial tool for setting forth the safety planning procedures. Following are some of the basic points to be developed under such a management plan. A preliminary SSPP is sometimes required at the proposal stage.

The system definition should not be limited only to central elements, but should also include an identification and definition of subsystems and internal and external elements that might have an effect on the system. This should provide the analyst with a comprehensive understanding of the system and the interactive nature of its elements. To give a safety program a definite direction, specific safety goals and objectives should be established. These objectives should cover both short-and long-range goals.

The next step should be to determine the organizational structure of the safety group, and to select and designate qualified personnel, assigning responsibilities respectively. System safety sometimes is overlooked or treated as an after thought unless it is given sufficient managerial visibility and entrusted to skilled and effective personnel.

In addition to having knowledge about the system, the analyst should enter into a preliminary hazard analysis. The purpose of such an analysis is to help develop design requirements used in the conceptual phases of the system's development. Data and experience acquired from older, analogous systems should be employed in determining preliminary hazards.

To insure effective and timely review and modification of the system safety objectives, milestones should be established. Milestones are formally designated points in a program, which are chosen for their prominent significance. Usually they are identified as crucial points in a program where progress is assessed and decisions made.

A description of methods to be used for the purposes of evaluating and monitoring the effectiveness and performance of the program should follow. A data base should be established and procedures for its collection and analysis defined.

In short, a preliminary system safety program should cover the following points:

- Define the system
- Set safety goals and objectives
- Determine organizational structure and responsibilities
- Identify, in preliminary fashion, hazards and their control
- Define and describe scheduling and review procedures (establish milestones)
- Describe methods for evaluating and monitoring performance
- Define data base and documentation requirements and procedures.

The preliminary system safety program plan uses elements of program management, to insure the accomplishment of the system safety tasks, including identification of the system safety requirements, planning and organization of the efforts directed toward the safety objectives.

The System Safety Program Plan in its final version is a document with more of a technical and engineering content than the preliminary SSPP. A checklist of requirements for a system safety program, as used today in the military and industry, is shown in Figure 2.

The evaluation of the safety program should be performed to assure compatibility with stated goals and objectives. Sometimes such assessments may lead to program realignment or goals redefinition. Once the system's boundaries have been defined, possible hazards identified, and objectives established, analytical techniques are employed to analyze the system and data on failure roles, repair roles, probabilities, and environmental conditions collected for the analysis.

There are many analytical and managerial techniques available for hazard identification and risk evaluation: Failure Mode and Effect Criticality Analysis, Fault Tree Analysis, Reliability Analysis, Risk Analysis, and Task Analysis are only some of the

1.0 PURPOSE AND SCOPE
2.0 APPLICABLE DOCUMENTS
    (Reference only documents cited in the plan text)
3.0 SAFETY ORGANIZATION
    3.1 Relationship in total organization
    3.2 Organizational array
    3.3 Responsibilities
    3.4 Interfaces

4.0 SAFETY TASKS TO BE COMPLETED
    4.1 Criteria development
    4.2 Analyses
    4.3 Design/program review participation
    4.4 Contractor/subcontractor requirements
    4.5 Reporting
    4.6 Documentation
    4.7 Planning
    4.8 Evaluations

5.0 METHODS FOR ACCOMPLISHING SAFETY TASKS
    5.1 Criteria-development, documentation and monitoring
    5.2 Analysis technique
    5.3 Other program activities

6.0 SCHEDULE FOR TASK COMPLETION
    (Keyed to major program milestones)

CHECKLIST OF REQUIREMENTS FOR A SYSTEM SAFETY PLAN

FIGURE 2

techniques used.

ANALYTICAL SAFETY TECHNIQUES

Following is a short description of some of those techniques which appear to be most promising for application to transportation:

Risk Analysis is a technique for quantifying the penalty in injuries, deaths and property damage, due to failures, involving the probability of an accident and its severity, providing a basis for setting quantitative safety goals. The comparison of social and individual risks, is extremely useful in the analysis of safety measures and facilitates trade-offs, subject to managerial decisions.

The difficulties with this approach are that there is no general agreement on the value of human life, and, while two different risks might have the same dollar value, society's reaction would greatly differ, depending upon whether the actual result is property damage, injury or fatality.

The Failure Mode and Effect Analysis (FMEA) is a systematic procedure for identifying the modes of failures and for evaluating their consequences. It is a tabular procedure which considers and depicts hazards in terms of single-event chains and their consequences. The FMEA is generally performed based on limited design information during the early stages of design, and is periodically up-dated to reflect changes in design and improved knowledge of the system. The basic questions which must be answered by the analyst in performing an FMEA are:

(1) How can each component or subsystem fail? (What is the failure mode?)
(2) What cause might produce this failure? (What is the failure mechanism?)
(3) Identifying potential failures and the magnitude of their efforts on the system.
(4) Developing testing and check-out methods.
(5) Providing a basis on which to build further qualitative reliability, availability, and safety analysis.
(6) Providing input data for construction of SBD and FTA models.
(7) Providing a basis for establishing corrective measures.
(8) Performing an objective evaluation of design requirements related to redundancy, failure detection systems, and fail-safe character.

The output of this analysis is a qualitative set of parameters which can be ranked and which relate levels of severity, probability of occurrence, and relative cost.

The Reliability Safety Block Diagram (RBD or SBD) is a success-oriented diagram which represents the logic of a system. SBD's are developed through analysis of functional relationships among various components and subsystems.

Large complex systems are analyzed and broken down into subsystems, carefully defining interrelationships among them. The process is continued until the subsystems are small enough for easy analysis and data availability.

Each of the blocks in an SBD represents the success of the safety-critical component or subsystems, and their interrelationship is expressed by the way in which the blocks are interconnected in the block diagram, thus pictorially representing various success paths. The success of any of these paths indicates system success, and produces a path from input to output. Probability theory is used to derive a probability of success expression from the diagram, based on an element's success/failure data.

Safety graphs (SG) and SBD's, are identical except for notation. Also, SBD and SG can be used to analyze safety or reliability; however, most analysts find them more convenient in reliability analysis, because they are success-oriented. Often a FMEA is used as an aid in constructing an SBD or an SG.

Fault Tree Analysis (FTA) is an application of deductive logic to produce a failure or fault-oriented pictorial diagram, which allows one to analyze system safety or reliability. Various failure modes that can contribute to a specified undesirable event are organized deductively and represented pictorially.

First the top undesired event is defined and drawn. Below this, sub-undesired events are drawn. These sub-undesired events include the potential hazards and failures that are immediate causes of the top event. Below each of these sub-events are drawn second-level events, which are the immediate causes of the sub-events. The process is continued until one reaches basic events (often called elementary faults). Since the diagram branches out, and there are more events at each lower level, it represents an inverted tree. The tree-like structure of the diagram illustrates the various critical paths of sub-events leading to the occurrence of the top undesired event.

The method lends itself to both qualitative and quantitative analyses. The quantitative evaluation of a fault tree is possible when probabilistic data of failure events is available.

Both FTA's and SBD's are useful, and

(1) They force the analyst to actively seek out failure events (success events in a deductive manner)

(2) They provide a visual display of how a system can fail, and thus aid understanding of the system by persons other than the designer.
(3) They point out critical aspects of systems failure (system success).
(4) They provide a systematic basis for quantitative analysis of safety or reliability.

Many analysts prefer to use FTA in safety problems because the failure-oriented approach seems more natural; however, SBD & FTA are mathematically equivalent. If an analysis is crucial, one can construct a SBD and a FTA and check the results.

Criticality Analysis provides a tool to measure the relative impact of basic events and rank them for corrective action priority. One way to accomplish criticality ranking is to assign weights based on the risk analysis to each failure mode found in the FMEA analysis. From the SBD or FTA, the probability of occurrence for each mode is computed. Three tables may then be produced, each failure mode by frequency, risk measure, or the product of risk measure and frequency.

Criticality ranking may be used to determine:

- which items should be given in-depth study for ranking elimination of a hazard
- which items require special attention during production
- special requirements to be included in specifications for suppliers or contractors
- where should special procedures, safeguards, monitoring warning systems be provided
- where could prevention efforts be applied more effectively

This method combined with the Failure Modes and Effects Analysis is sometimes called Failure Modes Effects and Criticality Analysis (FMECA).

ILLUSTRATIVE EXAMPLE OF SIMPLIFIED AUTO DRUM BRAKES

The example considers the braking system of a 1969 Ford, without power brakes or anti-skid brakes, and excluding the parking (emergency) brake and the dash warning light. An analysis at the detailed (piece-part)* level is a difficult task. The major subsystems in the braking system contain about 196 parts and assemblies as detailed in a dealers shop manual.*

The major subsystems and approximate parts counts are: pressure differential valve (8 parts), self-adjusting drum brakes (4x15 parts), wheel cylinder (4x9 parts), tubing, brackets and connectors (50 parts), dual master cylinder (22 parts), master cylinder installation parts (20 parts). Frequently, because of lack of data, analysis is not carried out at this piece-part level. Even with scanty data, an analysis is still important, since often it will show obvious weaknesses of such a braking system which can be improved when redesigning it. In such a case, redesign is warranted, based on engineering judgment, even without statistics on frequencies of the failure modes. The example will be performed at a higher level, and will group together all failure mechanisms which cause the particular failure mode in question.

An FMECA for the simplified braking system is given in Table I. Inspection of the table shows that the modes which most seriously affect safety are Nos. M2, M4, and M7, and the design should be scrutinized in a design review to assure that the probability of occurrence for these modes is minimized.

Failure Mode	Mechanisms	Safety Criticality	Comments
M1. Differential value - failure (1/2 system)	Leakage or blockage	Medium	Reduces braking efficiency
M2. Differential value - failure (Total system)	Leakage affecting both front and back systems	High	Loss of both systems
M3. Master cylinder failure (1/2 system)	Leakage or blockage	Medium	Reduces braking efficiency
M4. Master Cylinder failure (Total System)	Leakage (Front and back)	High	Loss of both systems
M5. Drum brakes Self Adjusting	Leakage or blockage of one assembly	Medium	Unbalance of brakes causes erratic behavior
M6. Tubing brackets and connectors (1/2 system)	Leakage or blockage	Medium	Reduces braking efficiency
M7. Pedal and linkage	Broken or jammed	High	Loss of both systems

A SIMPLIFIED BRAKING SYSTEM
FMECA
TABLE 1

The next step in analysis would be the construction of an SBD or an FT. Assume that a safety failure occurs if modes M2, M4, or M7 occur singly, and modes M1, M3, M5 and M6 occur in pairs. (Actually the paired modes must affect both front and rear systems to constitute a failure; but approximations are made here to simplify the analysis.) Based on the above assumptions, the SBD and FT given in Figures 3 and 4, respectively, are obtained. Given either the SBD of Figure 3 or the FT of Figure 4, an equation can be written for the probability of safety (or unsafety), using probability principles. Computer programs are used in complex cases; this simplified case can be written:

$P_s \cong$ Probability of a safe condition from Figure 3 =

$$P[(x_2 \cdot x_3 \cdot x_7) \cdot (x_1 \cdot x_3 \cdot x_5 + x_1 \cdot x_3 \cdot x_6 + x_1 \cdot x_5 \cdot x_6 + x_3 \cdot x_5 \cdot x_6)]$$

$P_u \cong$ Probability of an unsafe condition from Figure 4

$$P[(\bar{x}_2 + \bar{x}_4 + \bar{x}_7) + (\bar{x}_1 \cdot \bar{x}_3 + \bar{x}_1 \cdot \bar{x}_5 + \bar{x}_1 \cdot \bar{x}_6 + \bar{x}_3 \cdot \bar{x}_5 + \bar{x}_3 \cdot \bar{x}_6 + \bar{x}_5 \cdot \bar{x}_6)]$$

What is desired is the probability of an accident, P_A and of course each failure mode has a different probability of leading to an accident. For simplicity, all these probabilities are assumed to be the same, and are equal to 0.5. This means that

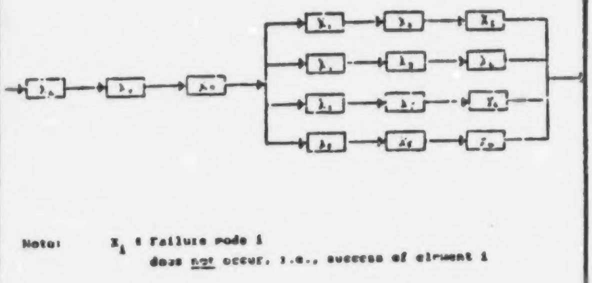
$$P_A = 0.5(1-P_s) = 0.5\ P_u$$

An analysis in more depth would require more detail (and more input data). The choice of how much decomposition to lower levels of detail is required in an analysis is often determined by data availability. To continue the analysis failure data on the modes M_1, $M_2 \ldots M_6$ is required. If, for M_3, the failure rate were constant and equal to λ_3 failures per mile, then the possibility of mode M_3 occurring or not occurring in M miles would be:

P(mode M_3 does not occur) = $P(X_3) = e^{-\lambda_3 M}$
in M miles

---

* 1969 Car Shop Manual, Volume 1, Ford Service Publication


Note: X_i = Failure mode i
does not occur, i.e., success of element i

SAFETY BLOCK DIAGRAM FOR
SIMPLIFIED BRAKE EXAMPLE
FIGURE 3

$$P\ (\text{mode } M_3 \text{ does occur in } M \text{ miles}) = P(\bar{X}_3) = 1 - e^{-\lambda_3 M}$$

To complete the analysis, the failure rate data λ_i is substituted into the equations to determine $P(X_i)$ or $P(\bar{X}_i)$, then these terms are substituted into the equations for P_s or P_u, and lastly, P_s or P_u are substituted into the expression for P_A.

The safety analysis consists of:

1. Decomposing the system into subsystems or pieceparts.
2. Drawing a safety block diagram (SBD) or fault tree (FT) (computer programs are available for this purpose)*.
3. Computation of the probability of safety or unsafety from the SBD or FT (computer programs are also available)* for this purpose.
4. Determine the failure rates of each component element. This is a data collection and estimation problem.
5. Substitution of failure rates into expression of step 3 (also done by computer programs)*.
6. Determination of probabilities of accident for each mode. (estimation from data)
7. Computation of probability of accident using the results of steps 5 and 6.

SYSTEM RELIABILITY, MAINTAINABILITY, AND AVAILABILITY

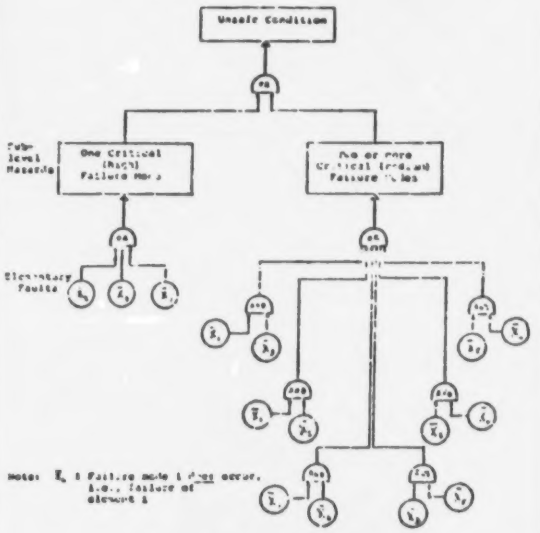
The techniques used in system reliability, maintainability, and availability analysis are, to a large extent, similar to those used in safety analysis. (FMEA, FMECA, RBD, FTA). The main difference is the definition of system reliability as system safety. For example, in safety analysis the concern is primarily with injury or death, and the application of an FMEA to an automobile would concentrate on critical sub systems such as brakes, suspension, steering, tires, collision restraint devices, and body/chassis protection. A reliability FMEA for an automobile would concentrate on high cost and frequently failing sub systems such as the power-train, ignition system, fuel system, lighting system, exhaust system, and preventative maintenance actions. The repair cost of accident damage to the auto body could logically be included in either analysis (as long as the definition of safety includes equipment and property damage).

Reliability is defined as the probability that a system or a part will satisfy its performance requirements for a time interval under actual use conditions. Reliability prediction is the process of estimating the probability, and is based on design information and historical data. Reliability can be optimized with respect to performance and other effectiveness factors. The estimating of reliability involves failure rate a function of time.

Most of the systems used are repairable, and therefore can be restored to service after a failure. Maintainability is defined as the probability that a failed system is restored to operable condition in a specified "down time", when maintenance is performed under stated conditions. "Down time" is the interval during which the system is not in operable condition and is comprised of (1) active repair time, (2) logistic time, and (3) administrative time.

Assessing maintainability is a form of applied probability analysis. Maintainability analysis for a system is related to queueing.

From the equipment viewpoint, it is important to study not only its probability of success (reliability) but the probability that the system is up (working) i.e., the availability of the system. In many cases, safety related equipment is on standby, and is under repair and down for certain periods of time during operation. In most cases the probability of an accident will depend on compound events e.g., the probability that the traffic light is not working times the probability of an accident given the traffic light is not working. An availability model would be used to compute the former probability.


Unsafe Condition
OR
Sub-level Hazards
One Critical (High) Failure Mode
Two or more Critical (reduced) Failure Modes
OR
OR
Elementary Faults
AND
AND
AND
AND
AND
AND
Note: $\bar{X}_i$ = Failure mode i does occur, i.e., failure of element i

SAFETY FAULT-TREE FOR
SIMPLIFIED BRAKE EXAMPLE
FIGURE 4

---

*The NASA-RBD computer program based upon the Messinger/Shooman algorithm (see Chapter 7 of NASA,CR- 1129 Report,"Practical Reliability", Aug. 1968) and the AEC-FTA computer program (PREP/KITT/TREBIL) used in connection with the Rasmussen Nuclear Reactor Safety Study WASH-1400.

The mathematical technique generally employed in computing availability is the Markov model. Of the above techniques it would appear that Risk Analysis, Failure Mode Effects Analysis, and Fault Tree Analysis hold the greatest promise for applicability to common transportation modes, based on their ease of comprehension and utilization by technical and managerial personnel in transportation.

The loosely structured tabular formats, such as FMEA, are more suitable for systematic, qualitative identification of potential hazards and their causes, consequences, evaluations, and corrections. This format also relies less on analytical expertise than does a focused logic diagram such as Fault Tree Analysis.

HUMAN FACTORS

There is still a question of the applicability of these techniques to the human aspects of transportation safety, which have not been explored to any great degree.

It is apparent that applications to System Safety in the field of human factors should involve a number of areas, including

- Behavior Theory
- Task Analysis
- Human Error Analysis
- Information Processing
- Comfort, Convenience, and Safety

Most studies of human factors have concentrated on two major areas: the military/NASA, and the automotive industry. In the first case, the subject of study is a highly trained, highly motivated person controlling an extremely complex mechanism. The human then becomes an element in the mechanical system, with limited, but necessary decision-making powers, and a need for high-level physical responses. In the second case, the subject of study is a minimally trained, unmotivated (for the specific task at hand) person in relation to a relatively simple mechanism (in comparison). This "man-machine system" has an almost infinite number of combined response possibilities to the many stimuli involved in the driving task. Between these extremes lie all other transportatiion modes, in descending order of relative complexity, perhaps, from air to sea to rail to motor vehicle.

Added to these considerations is the fact that the highway or motor vehicle mode, is one composed almost entirely of non-"professional" (and thereby relatively untrained) operators, only comparable to the much smaller group of small-boat operators in the marine area.

Studies to date have overwhelmingly been directed at the operator (pilot, engineer, driver) of a vehicle, with little or no effort expended on other humans involved in a transportation-related task, such as design, engineering and maintenance, or in various roles such as passenger, or bystander.

MANAGERIAL TECHNIQUES

Another area of system safety not discussed here is that of the application of managerial techniques to the implementation of a system safety program. These include:

- cost-effectiveness analysis
- organizational structures
- job analysis
- selection, training, and certification of personnel
- testing and certification of equipment
- contracting procedures

It was not the intent of this paper to cover human factors or managerial techniques, but to point to some of the existing technical methods available for safety analysis which are only now being applied to transportation.

The authors are currently involved in a USDOT project entitled "System Safety - An Interdisciplinary Approach to Transportation Safety", directed to the identification and application of existing system safety technology to the transportation field. As this project progresses, a greater emphases is expected on the applicability of these techniques to the human element.

CONCLUSION

Through the use of a systematic approach to safety, potential hazards can be identified before they are activated. The thrust of a system safety approach is oriented towards action rather than reaction. This is one of the main differences between the classical conservative approach to safety and the dynamic system safety approach discussed above. Accidents can be prevented, if necessary and adequate action is taken to eliminate and control hazards. A system safety approach does not imply that that systems must be risk-free, but rather that risks can be controlled and known to management. Thus, the resources needed to design or redesign a transportation system to meet specified risks, can be estimated at the outset and refined as work progresses. Development of data to support managerial decisions may be seen as the real role of system safety.

BIBLIOGRAPHY

1) Ericson, C.A., System Safety Analytical Technology-Fault Tree Analysis, The Boeing Company, 1970.

2) Farish T.P., System Safety Criteria For Use in Preparation or Review of Procedures, NASA TM x-5366-, October [illegible].

3) Goldsmith A., Guide to System Safety Analysis in the Gas Industry, II. Research Institute

4) Hammer W., Handbook of System and Product Safety, Prentice Hall Inc., Englewood Cliffs, N.J. 1972.

5) Lambert H., Fault Tree Analysis - An Overview Laurence Livermore Laboratory, University of California, 1974.

6) NASA CR-1126, Practical Reliability, Volumes I, II, III, IV, Research Triangle Institute, 1968.

7) Preparation of a System Safety Program Plan for Aviation Systems Development, Techinical Research and Applications Department, USAAAVS, 1972.

8) Risk Concepts in Dangerous Goods Transportation Regulations., NTSB Special Study, Washington, D.C.

9) Shooman M., Probabilistic Reliability - An Engineering Approach, McGraw Hill, 1968.

10) System Safety - Design Handbook, AFSC DH 1-6 Fourth Edition, 1974.

11) System Safety Engineering, SAMSO Manual, 1973.

12) System Safety Program for Systems and Associated Subsystems and Equipment, Military Standards - 882, 1969

13) *System Safety - Volume 3*, NASA Safety Manual, 1970.

14) "Techniques of System Reliability Prediction" (Using the Automobile as an Example), Proceedings the 1971 Annual Symposium on Reliability and Maintainability.

15) WASH-1400, *Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants*, 13 Volumes, U.S. Atomic Energy Commission, August 1974.

APPENDIX D

COMPENDIUM OF HAZARD ANALYSIS TECHNIQUES

A COMPENDIUM OF HAZARD IDENTIFICATION AND EVALUATION TECHNIQUES FOR SYSTEM SAFETY APPLICATION

by P.L. CLEMENS, P.E., CSP

Purpose

In the arena of system safety, a large number of techniques have emerged for use in identifying and in evaluating hazards. These many techniques are well described in scattered references. However, no single document describes – or serves as a guide to – more than a few of them.

This compendium has, as its purpose, the compilation of brief descriptions of 25 of the hazard identification and evaluation techniques which are often cited in the literature and are often employed by modern system safety practitioners. For each technique, one or more references are listed in which further information describing its methodology and application can be found. An attempt has been made to list only the most prestigious references and to reduce rather than to expand their number; the purpose in this has been to aid the engineer who might wish to build a library of references which is adequately comprehensive but not overly voluminous.

For the most part, these many hazard discovery and evaluation techniques should be viewed as complementary rather than as competitive. Hazards which may go undetected by one technique may be uncovered by others. This, in fact, is one characteristic of the techniques – and indeed of the practice of system safety itself – which has led to their proliferation.

This compendium is incomplete. It is axiomatic that any such compilation as this *will* be incomplete; such techniques as these can be produced in a variety which has no limit other than that imposed by the imaginations of those who produce the techniques. Omissions from this compilation include, for example, Critical-Path Analysis, Man-Path Analysis, and Technique for Human Error Rate Prediction (THERP).

Alternatively, some techniques have been included here not because they amount to discretely unique analytical methods, but because their prevalence in the literature warrants it. An example is the Preliminary Hazard Analysis. Such an "analysis" is not so much a discrete technique as it is the application of *any* technique, or any group of them, performed *preliminarily* – e.g., *prior* to design or *prior* to initial operation.

Finally, it is not to be assumed that an effective system safety program must make use of all of these techniques, nor that a program necessarily becomes more effective by an increase in the number of techniques that it does use. Rather, the well formulated program will have considered many such techniques – those described here, and others as well – and will have adopted those which yield the best risk-control benefits in the particular environment and in return for the resources which are available for the practice of system safety.

Information Presentation

Twenty-five hazard identification and evaluation techniques are described in this compendium. A common method of information presentation has been applied to each, in order to facilitate comparisons and selections. The method of information presentation follows this pattern:

Method: A succinct statement of the process which must be followed to apply the technique is provided. This description is a digest of information drawn from the references, coupled with advice from those who have practiced the use of the technique.

References: Identified here are the formal publications from which descriptive information has been drawn. These references are listed elsewhere, and the rationale for their selection is described under *Purpose.*

Application: Special system/subsystem/component areas to which the technique may be applicable are noted, as are processes/activities/procedures. Areas of *in*applicability are also delineated, where this has been appropriate. Techniques which are especially applicable to *manned* systems, activities and procedures are so identified. (Objective descriptions of areas of application are difficult to assemble for all but the more highly specialized techniques; the practitioners of a given technique are inclined to have developed diversified methods for using it which will have given it the appearance of being universally applicable.)

Thoroughness: By their nature, some techniques are well suited to broad and/or rapid, superficial studies. Others lend themselves to finely detailed, in-depth explorations. Comments on these aspects of thoroughness are provided.

Mastery Required: Some techniques lend themselves to easy application by the untrained novice, whereas others may require formal study and some practical experience. An attempt has been made to indicate the degree of preparation required for the successful use of each technique.

Difficulty of Application: Presuming that a given technique has been adequately mastered and that it is not mis-applied, its use may produce acceptable results either with relative ease or at great expense in time and resources. Comments on these features are provided here.

Comments: Miscellaneous notes and precautions drawn largely from discussions with practitioners of the techniques are presented, where applicable.

The Techniques

The pages which follow present each of the 25 system safety hazard identification and evaluation techniques which are treated in this compendium.

Change Analysis (Ref. 10)(Ref. 12)

Method: Consider existing, known system as a baseline. Examine the nature of all contemplated or real changes, and analyze the probable effect of each change (singly) and all changes (collectively upon system risks.

Application: Although originally conceived for management system applications, Change Analysis has come to be applied to systems of all kinds. It can *only* be applied, of course, if system design change or actual alteration has occurred or is contemplated. It is well applied as a means of optimizing the selection of a preferred change from among several candidate changes, or in aiding the design of a needed change. The technique can be applied meaningfully only to a system for which baseline risk has been established (e.g., as a result of prior analysis).

Thoroughness: Thoroughness is constrained, quite obviously, only by the depth/detail treated in performing the analysis. Thoroughness *required* to analyze a given change, equally obviously, is governed by the extent of the change itself. Effectiveness *cannot exceed* that of prior analysis(es) used in establishing baseline risk.

Mastery Required: Understanding of the physical principles governing behavior of the system being changed is essential, in order that the effects of the change can be determined with confidence adequate to the purposes of the analysis. Assuming that the complexity of the changes does not appreciably exceed that of the system prior to alteration, mastery of the baseline analytical technique becomes sufficient.

Difficulty of Application: Difficulty is determined largely by the extent to which the system has undergone (or will undergo) change, in combination with system complexity.

Comments: Chief advantage of the technique lies in its "shortcut" approach: i.e., only the effects of change(s) need be analyzed, rather than the system as a whole. In this advantage also lies the technique's chief shortcoming: i.e., the presumption that the baseline analysis(es) have been carried out adequately.

Contingency Analysis (Ref. 1, pp 158-209)(Ref. 8, p 481)

Method: Identify the credible mishaps that might occur in a given system, and examine the existence and adequacy of emergency measures and protective equipment with which control can be established and/or harm can be avoided in the event of each credible mishap.

Application: Contingency Analyses may be applied universally to all systems, subsystems, components, procedures, interfaces, etc. To satisfy the definition, they must be performed for the specialized purpose of examining the existence and the suitability of system contingency features. In general system applications, the Contingency Analysis may be considered as an effective means to aid in disciplining the approach to evaluating the adequacy of back-up elements and/or control paths intended to mitigate failures. It is also of particular value in assessing the adequacy of disaster response plans and equipment.

Thoroughness: Thoroughness is determined largely by (1) the degree to which mishap modes have been identified and (2) the adjunct technique(s) employed to examine the existence and adequacy of mitigation features within, or available to, the system. (See *Comments*, below.)

Difficulty of Application: Selection of technique(s) to be used determines difficulty of application. (See Comments, below.)

Comments: The Contingency Analysis is not a discrete technique. Instead it is the application of any technique, or any group of them, performed for the specific purposes of determining the need for, the existence of, and the adequacy of system contingency features.

Critical Incident Technique* (Ref. 1, pp 190-192)(Ref. 7, pp 100-102)

Method: Interview operationally experienced personnel (and/or use questionnaires) to collect information on past mistakes, hazards and near misses. Identify dominant/high-risk cases.

Application: The technique may be applied, without restriction, to any system having human operators or observers, for which a reasonable background of historical operational experience has been accumulated.

Thoroughness: The technique is limited in thoroughness by (1) the degree to which near misses which are likely ultimately to result in, or to contribute to, a critical incident will have been experienced and (2) the fidelity with which those instances will have been noted, remembered, and reported by competent operators or observers.

Mastery Required: Expertise at gathering objective data from subjective interviews in a sine qua non. Beyond that, a grounding in the principles of system safety and risk assessment are necessary.

Difficulty of Application: Given proper preparation (see *Mastery Required*, above) application of the technique is straightforward and uncomplicated.

Comments: This technique has come to enjoy a more favorable reputation than the other "what-if" methods; cf. Scenario and Maximum Credible Event/Worst-Case Condition.

Criticality Analysis (Ref. 1, pp 156-159)

Method: Rank the damage potential of system elements according to a scale which represents the harm each might cause, upon failure.

Application: The technique is universally applicable to all systems, processes, procedures and their elements.

Thoroughness: Thoroughness can only be regarded as absolute; i.e., for each failed system element considered, a damage potential ranking (or rankings) can be produced. *Identification* of the specific failures to which the Criticality Analysis is to be applied, however, must be accomplished by an adjunct technique (e.g., Failure Modes & Effects Analysis), hence will rely upon the thoroughness achievable by that technique.

Mastery Required: A variety of arbitrarily formulated criticality indices exist in the literature for use in coding the loss potential of failures. The ability to apply these scalar indices to specific practical cases is acquired with relative ease.

Difficulty of Application: Application is readily accomplished for cases in which failure modes have been identified. However, use of Criticality Analysis is practical, system cases must pre-suppose that the specific failures to which it is to be applied have been identified. If they have not, application of an adjunct technique then becomes a necessity, and the difficulty of applying the adjunct technique predominates.

Comments: This technique is quite often combined, in practice, with the Failure Modes and Effects Analysis.

Energy Analysis (Ref. 1, pp 159-164)(Ref. 5, pp 25-40)

Method: Identify all sources of energy within a system, and examine the adequacy of barriers to the unwanted flow of that energy to "targets" which might suffer harm.

Application: The technique can be applied to all systems which contain, make use of, or which store energy in any form or forms (e.g., potential or kinetic mechanical energy, electrical energy, ionizing radiation, chemical energy, thermal energy, etc.). In conjunction with other techniques, Energy Analysis is applicable also to systems which *control* the containment, use, storage or flow of energy. The technique is *inapplicable* – without use of special interpretations – to the discovery and analysis of hazards which are not energy-related, and exclusive reliance upon its use can leave important hazards undiscovered (e.g., the presence of asphyxiants in confined spaces).

Thoroughness: The likelihood of oversight in cataloging the sources of energy within a system is small. (Checklists are available in the literature as aids to the process.) The likelihood of oversight in identifying system vulnerability to *external* sources of energy can be great, however. The effects of *rates* of energy application and of frequency or total number of cycles of application are sometimes overlooked (e.g., shock loading and fatigue), as are *combined* energy effects (e.g., a vessel whose walls are simultaneously exposed to a pressure differential and a thermal gradient).

Mastery Required: Inconsequential preparation is required for cataloging energy sources within a system. However, use of the method also requires recourse to the expertise needed to judge the adequacy of barriers to the unwanted flow of that energy.

Difficulty of Application: The cataloging of energy sources is carried out with relative ease. Gaging the adequacy of static barriers can be accomplished, in many cases, by simple comparison of the physical characteristics of the system with requirements levied by codes, regulations and standards. (Ordinarily, this will have been done and documented during system design.) Application becomes more difficult in systems wherein process controls play a part in restraining the unwanted flow of energy. The adequacy of such controls – whether automatic or manned – is not amenable to straightforward analysis by this technique, and other methods must be used to support it.

Comments: The method is of special value as a quickly applied "first-look" technique. It is inclined to focus exclusively upon energy sources *within* the system being analyzed. External sources (e.g., from adjacent systems or forces of nature) are often overlooked. When applied in the making of "safe-to-enter" decisions, special adaptations are necessary to ensure that, although the environment is free from unrestrained sources of energy likely to cause harm, it will support life.

Event-Tree Analysis* (Ref. 13, p. 62)

Method: Select *initiating events*, both wanted and unwanted and develop their *consequences*, both wanted and unwanted, through consideration of system/component failure-and-success alternatives. Continue through all alternate paths, considering each consequences as a new initiating event.

Application: The technique is universally applicable to systems of all kinds, with the limitation that unwanted events (as well as wanted events) must be anticipated to produce meaningful analytical results.

Thoroughness: The technique can be exhaustively thorough. Thoroughness has only two theoretical limits:

---

*"Critical Incidents" are known to the Department of Energy as "Reported Significant Observations," or "Unusual Operating Reports."

*Ref., Fault-Tree Analysis and Network Logic Analysis.

the presumptions that (1) all system events have been anticipated, and that (2) all consequences of those events have been explored.

Mastery Required: The technique is among the more difficult. Successful application to complex systems cannot be undertaken without formal study over a period of several days to several weeks, combined with some practical experience.

Difficulty of Application: Once mastery is achieved, the technique is not particularly difficult to apply. It is, however, enormously time consuming. It must be recognized that the exploration of all *wanted* events and their consequences – as well as *un*wanted ones – increases the effort substantially beyond that required for Fault-Tree Analysis or for Failure Modes and Effects Analysis.

Comments: Of the techniques presented in this compendium, Network Logic Analysis, Event-Tree Analysis and use of the Naked Man principle are beyond question the most exhaustive, properly applied. Axiomatically, their use also consumes large quantities of resources. Their use, therefore, is well reserved for systems wherein risks are thought to be high and well concealed (i.e., not amendable to analysis by simpler methods).

Failure Modes & Effects Analysis* (Ref. 1, pp 148-156)(Ref. 8, pp 466-468)

Method: Examine system, element by element. Identify modes in which each element can fail. Determine effect(s) upon system of each failure mode, taken both singly and in combination with others. (Some variations classify effects according to their severity.*)

Application: The technique is universally applicable to systems, subsystems, components, procedures, interfaces, etc. (When applied to procedures, they must be sufficiently documented or otherwise formalized as to lend themselves to the necessary analysis – cf. Procedure Analysis.)

Thoroughness: Thoroughness is dictated by: (1) the degree to which failure modes are identified and explored, (2) the degree to which effect "avenues" are identified and to which they are explored, for *each* failure mode, and (3) the degree to which the effects of *multiple, co-existent* failure modes are analyzed.

Mastery Required: Mastery for the uninitiated, seeking to analyze systems of more than trivial complexity, requires from several days to several weeks of formal instruction or study, and practical experience. Working knowledge of Boolean algebra is helpful.

Difficulty of Application: Once mastery is achieved, the technique is not particularly difficult to apply. It is, however, enormously time consuming. Although only *failure* modes (e.g., component faults) are explored – unlike Event-Tree Analysis – both those failure modes which will and those which will not result in great harm must be entertained to develop the analysis fully.

Comments: The technique has been highly regarded, but its application appears to be diminishing in favor of the less-time-consuming Fault-Tree Analysis. Over that latter method, this technique enjoys the advantage that no undesirable event need be predetermined to enable its use.

Fault-Tree Analysis* (Ref. 1, pp 238-246)(Ref. 4, pp 18-20)(Ref. 8, pp 468-475)(Ref. 11, Section 5.5.1.2.b)(Ref. 12, pp 208-211)(Ref. 14)

Method: Identify an undesirable event and the contributing elements (faults/conditions) that would precipitate it. Interconnect the contributors and the undesirable event, using network paths through Boolean logic gates.

Application: The technique is universally applicable to systems of all kinds, with the limitations that (1) the undesirable system events which are to be analyzed/abated, and their contributors, must be foreseen and (2) each of those undesirable system events must be analyzed individually.

Thoroughness: Chief limitations of the technique are: (1) the presumption that the relevant undesirable events have been identified, and (2) the presumption that contributing factors have been adequately identified and explored in sufficient depth. Apart from these limitations, the technique as usually practiced is regarded as among the most thorough of those prevalent for general system application.

Mastery Required: Mastery for the uninitiated requires from eight to 40 (or more) hours of study and some practical experience. Prior knowledge of Boolean algebra and/or the use of logic gates is helpful.

Difficulty of Application: Application, though time-consuming, is not difficult once the technique has been mastered. Computer aids are available and are increasingly used. Unlike Event-Tree Analysis and Failure Modes & Effects Analysis, the technique explores only those faults and conditions leading to intolerable losses.

Comments: The method is capable of producing numerical statements of the probability of occurrence of undesirable events, given probabilities of contributing factors. That capability leads to a common abuse: much effort can be expended in producing "refined" numerical statements of probability, based on contributing factors whose individual probabilities are poorly known and to which broad confidence limits should be attached. As marked advantages, the method identifies minimum sets of contributing factors which, if they can be prevented, will prevent the occurrence of the central, undesirable event. Similarly, it identifies minimum sets of contributing factors which, if they occur, will invariably precipitate the central undesirable event. Common causes and human operator paths to undesirable events are also disclosed by use of the method.

Flow Analysis* (Ref. 1, pp 168-170)

Method: Consider the confined or unconfined flow of fluids or energy – intentional or unintentional – from one component/subsystem/system to another. Find and evaluate opportunities for that flow to occur without intended constraint, in ways which might result in harm.

Application: The technique is applicable to all systems which transport, or which control the flow of, fluids or energy. Adjunct techniques are often essential to success in the use of Flow Analysis (e.g., in analyzing fluid flow control systems to determine unwanted modes of flow and their probabilities).

Thoroughness: The likelihood of oversight in cataloging intentional flows of fluids or energy within a system is small. The likelihood of oversight in identifying opportunities for *unintentional* flows is great, however. Even greater is the likelihood of oversight in identifying opportunities for *combined* unintentional flows.

Mastery Required: Inconsequential preparation is necessary to enable a straightforward cataloging of the intentional flows of fluids or energy within a system. However some expertise must be acquired at judging the adequacy of barriers to unintentional flows. If adjunct techniques are to be used (see *Application*, above) they must also be mastered.

Difficulty of Application: The cataloging of energy and fluid flows within a system is carried out with relative ease. Gaging the adequacy of static barriers can be accomplished, in many cases, by simple comparisons of the physical characteristics of the system with requirements levied by codes, regulations and standards. Application becomes more difficult in systems wherein process controls play a part in restraining the undesired flow of fluid or energy. The adequacy of such controls – whether automatic or manned – is not amendable to straightforward analysis by this technique, and adjunct methods must be used to support it.

---

*Variations are called by other names, e.g.: "Failure Modes, Effects and Criticality Analysis"; Ref. 2.

*Ref., Event-Tree Analysis and Network Logic Analysis.

*Ref., Energy Analysis.

Comments: This technique is inclined to focus exclusively upon fluid and energy flows *within* the system being analyzed. External sources of such flow (e.g., from adjacent systems or forces of nature) are often overlooked.

Interface Analysis* (Ref. 1, pp 164-168)

Method: Seek physical and functional incompatibilities between adjacent/interconnected/interacting elements of a system which, if allowed to persist under all conditions of operation, would generate hazards which could result in mishaps.

Application: Interface analysis is universally applicable, above the least-component level, to systems of all kinds. Interfaces treated may be inter-machine, intra-machine, man-machine, etc. without restriction.

Thoroughness: Thoroughness is determined by the extent to which interfaces are known (or can be anticipated) and the degree to which candidate incompatibilities can be identified. Thoroughness increases as additional, adjunct techniques are brought to bear to support Interface Analyses. (See *Comments*, below.)

Mastery Required: Understanding of the physical principles underlying the behavior of the interconnected system elements is essential. Mastery of adjunct techniques, if they are to be used to support the analysis (see *Comments*, below) is an obvious requirement.

Difficulty of Application: Difficulty is determined by system complexity and by the nature of such adjunct techniques as may be used. (See *Comments*, below.)

Comments: Use of adjunct techniques to support Interface Analysis is markedly beneficial – e.g., application of Failure Modes and Effects Analysis at each of many intra-system interfaces can serve to identify incompatibilities not discovered through Interface Analysis alone. A principal weakness of Interface Analysis lies in the presumption that incompatibilities between system elements can be identified, prior to failures, for all conditions of operations.

Job Safety Analysis (Ref. 2, pp 89-96)(Ref. 7, pp 110-116)

Method: Analyze job (or work process/system/operation) element-by-element, identifying hazards associated with each element. (Classically, this is done by a worker-supervisor-safety engineer team.)

Application: The technique is applicable to – and limited to – human operator functions. Those functions must be proceduralized in ways which provide assurance that they will not vary in significant ways, or anticipated variations in them must be accounted for in the analysis.

Thoroughness: Thoroughness is limited by: (1) degree to which job elements are explored, and (2) degree to which variations in/from procedural job elements are considered.

Mastery Required: Elementary analyses may be performed by the uninitiated analyst. More complex jobs, having many possible variations in job elements, require use of formalized techniques and training/experience commensurate with the complexity.

Difficulty of Application: The technique is quite readily applied to jobs having little opportunity for variation in the structure of individual job elements, but becomes difficult to apply when such variation exists and must be taken into account. (If such variation exists and is not taken into account, thoroughness suffers.)

Comments: Job Safety Analysis is widely regarded as a useful technique with which to identify hazards associated with human operations. Its use in the realm of industrial safety substantially antedates its system safety adoption.

Management Oversight & Risk Tree Analysis (Ref. 5)

Method: Apply a pre-designed, systematized logic tree to the identification of total system risks, both those inherent in physical equipment and processes and those which arise from operational/management inadequacies.

Application: The pre-designed tree – intended as a comparison tool – generally describes all phases of a safety program and is applicable to systems and processes of all kinds. The technique is of particular value in accident/incident investigation as a means of discovering system or program weaknesses or errors which provide an environment conducive to mishaps.

Thoroughness: Design of the "model" tree, against which comparison judgments are made, is exhaustively complete. As a result, thoroughness is limited only by the degree to which the analysis explores the existing or contemplated system, in mirroring it against the model tree.

Mastery Required: One day of formal instruction leads to capability at applying the technique. One-week courses, including diverse exercises in practical application, are seen as preferable.

Difficulty of Application: Although tedious and time-consuming, the technique is not difficult to apply once mastery is achieved (see above). Graphic aids and explanatory texts are available.

Comments: Popularity of the technique for application in accident/incident investigation is increasing.

Maximum Credible Accident/Worst-Case Condition* (Ref. 1, pp 66-67)

Method: Visualize the most severe mishap that might reasonably be expected to arise for a system. Consider all potential contributors to the mishap, in their worst-case states, and examine the reasonableness that the mishap itself might evolve as a result of their occurrence.

Application: The technique has universal application to systems and subsystems of all kinds, whether manned or unmanned.

Thoroughness: The technique lacks thoroughness chiefly to the degree that it relies upon the exercise of intuitive skills at imagining the nature of sometimes-complex events not yet experienced. A converse argument, favoring thoroughness, can also be raised: use of the technique induces consideration of system failures for which no historical basis is at hand.

Mastery Required: The technique is often practiced with success by the newly initiated novice. (See cautionary note under *Comments*, below.)

Difficulty of Application: Application is accomplished with little difficulty, presuming that the practitioner is adequately versed in the system and its environment of use.

Comments: Spontaneity of thought is essential to the practice of the technique. That same spontaneity can give rise to the visualization of "worst cases" which lack reasonable credibility. The practitioner must guard against uselessly expending resources in pursuing analyses of conceivable but incredible cases.

Naked Man (Ref. 6, pp 67-69)

Method: Consider the "primordial" system, with all existing safety features and mishap countermeasures removed. Examine theoretical base-line hazards in that state, and determine which ones are eliminated or appropriately suppressed – or which new ones might be added – as existing countermeasures are restored or new ones are applied.

---

*This technique is indistinguishable from the System Hazard Analysis.

*Ref., Scenario.

Application: The technique is universally applicable to systems and subsystems, whether manned or unmanned. It is recognized as especially useful in developing and/or analyzing confined-space entry safeguards and procedures.

Thoroughness: The technique tends to be exhaustively thorough, unless practiced superficially.

Mastery Required: Use of the system is readily mastered, requiring less than one day of instruction and practice with demonstration cases.

Difficulty of Application: Assuming the availability of a sufficiently detailed logging and documentation system, the technique is readily applied. It is, however, enormously time consuming.

Comments: Of the techniques presented in this compendium, Network Logic Analysis, Event-Tree Analysis and use of the Naked Man principle are beyond question the most exhaustive, properly applied. Axiomatically, their use also consumes large quantities of resources. Their use, therefore, is well reserved for systems wherein risks are thought to be high and well concealed (i.e., not amendable to analysis by simpler methods).

Network Logic Analysis* (Ref. 1, pp 229-237)

Method: Describe system operation as a network of logic elements, and develop Boolean expressions for proper system functions. Analyze the network and/or expressions to identify elements of system vulnerability to mishap.

Application: The technique has universal application to all systems, whether manned or unmanned, having components and/or operations which can be adequately represented in bi-modal elemental form.

Thoroughness: The technique can be exhaustively thorough. Thoroughness rests on the degree to which systems components and/or operations will have been represented in network form. (*Note:* peripheral service failures – e.g., utilities – and interface effects are often overlooked in the application of this technique.)

Mastery Required: The technique is among the more difficult. Working knowledge of Boolean algebra is essential. Successful application to complex systems cannot be undertaken without formal study over a period of several days to several weeks, combined with some practical experience.

Difficulty of Application: Once mastery is achieved, the technique is not particularly difficult to apply. It is, however, enormously time consuming. Because the technique explores all *wanted* as well as *un*wanted system performance eventualities, it requires substantially more effort than does Fault-Tree Analysis or Failure Modes and Effects Analysis.

Comments: Of the techniques presented in this compendium, Network Logic Analysis, Event-Tree Analysis and use of the Naked Man principle are beyond question the most exhaustive, properly applied. Axiomatically, their use also consumes large quantities of resources. Their use, therefore, is well reserved for systems wherein risks are thought to be high and well concealed (i.e., not amendable to analysis by simpler methods).

Operating & Support Hazard Analysis (Ref. 11, Section 5.5.1.4)

Method: Indistinguishable from Procedure Analysis.

Application: Same as for Procedure Analysis.

Thoroughness: Same as for Procedure Analysis.

Mastery Required: Same as for Procedure Analysis.

Difficulty of Application: Same as for Procedure Analysis.

Preliminary Hazard Analysis (Ref. 8, pp 464-466)(Ref. 11, Section 5.5.1.1)

Method: As a broad, initial study, identify apparent hazards, feasibility of controlling them, and methods which might be applied to effect the control. (Checklists are often used.) Alternatively, apply any hazard analysis techniques, singly or in combination, very early in system life cycle, preferably during formulation of design concept.

Application: Preliminary hazard analyses may be applied universally to all systems, subsystems, components, procedures, interfaces, etc. To satisfy the definition, they must be performed *preliminarily* – i.e., prior to or as an initial step of design, shakedown, operation, maintenance, refurbishment, etc.

Thoroughness: Thoroughness depends upon the technique(s) used and the depth to which they are employed. (See *Comments*, below.)

Mastery Required: Acquiring competence is dependent upon the technique(s) selected with which to perform the Preliminary Hazard Analysis. (See *Comments*, below.)

Difficulty of Application: Selection of technique(s) to be used determines difficulty of application. (See *Comments*, below.)

Comments: The Preliminary Hazard Analysis is not a discrete technique. Instead, it is the application of any technique, or any group of them, performed preliminarily – e.g., prior to the specific life cycle phase to which that analysis applies.

Procedure Analysis* (Ref. 1, pp 192-198)(Ref. 8, pp 476-481)

Method: Review, step-by-step, the actions that must be performed (generally in relation to mission tasks, equipment that must be operated, and the environment in which personnel must exist) seeking possibilities of mishaps as a result of those actions, e.g.: (1) the possibilities of harm to operators by the systems, and (2) the possibilities of harm to the system by the operators.

Application: Application is limited to systems involving procedures followed by human operators. Those procedures must be sufficiently documented, or otherwise formalized, as to lend themselves to the necessary analysis with reasonable confidence that the step-by-step protocol will not be violated. Alternatively, additional analyses must be performed to evaluate the effects of protocol violation.

Thoroughness: Thoroughness is limited by: (1) degree to which procedural steps/sub-elements are explored, and (2) degree to which error options are considered (e.g., imbedded) step performed out of sequence, step omitted, false step inserted.)

Mastery Required: Elementary analyses may be performed by the uninitiated analyst. More complex procedures having many error avenues require use of formalized techniques and training/experience commensurate with the complexity.

Difficulty of Application: The method is quite readily applied to operations having few error options, but becomes difficult to apply when multiple error options must be considered, or when single error options at multiple points in time or at separated operating stations must be dealt with in combination.

---

*Ref., Fault-Tree Analysis and Event-Tree Analysis.

*Procedure Analyses are often designated by the activity to be analyzed, e.g.: "Test Safety (Hazard) Analysis," "Operation Safety (Hazard) Analysis," "Maintenance Safety (Hazard) Analysis." – cf., Job Safety Analysis.

Prototype (Ref. 1, pp 170-180)

Method: Construct and operate, under widely varying conditions, system/subsystem mock-ups/models, and examine operation for evidence of failure under appropriately varied operating conditions.

Application: The technique is applicable to systems, subsystems and components, whether electrical/electronic or mechanical. Man-machine systems are also analyzed in prototype versions – e.g., using operational simulators. The validity of system replication is often questionable in such cases, however, particularly where operator stress is a factor requiring analysis.

Thoroughness: Thoroughness is dependent entirely upon the degree of system replication achieved in the construction and operation of the prototype.

Mastery Required: A finely detailed understanding of the system and its intricacies is essential in order for it to be modeled effectively in prototype version.

Difficulty of Application: Prototype analysis tends to be costly in resources and time, and is especially so at levels above the subsystem. For that reason, its application is customarily reserved for suspected high-severity cases which are not amendable to to adequate treatment by other techniques.

Comments: Manned control functions for mass transportation systems are often dealt with in prototype, using simulators which also serve as training devices.

Scenario* (Ref. 3, pp 11-12)

Method: Amass spontaneous ideas (often by members of a group) describing conceivable accidents and/or their contributors. Discard those deemed wholly unreasonable, and pursue the remainder by refining descriptions of their causes and consequences and judgments of their likelihood.

Application: Manned and unmanned systems and subsystems are amendable to treatment by this technique. The technique is of special worth in cases where system features are novel and, as a result, there is no historical data base for guidance or comparison.

Thoroughness: The technique is limited in thoroughness only by the ability of the practitioner to conceive of mishaps and of combinations of events, conditions and actions that might induce them.

Mastery Required: An unfettered mind and an active imagination lead to mastery. (It can be argued that overfamiliarity with the system under analysis restricts the freedom of thought processes necessary to successful application.)

Difficulty of Application: Application is accomplished with ease in all but obscure cases.

Comments: Because the method relies upon spontaneity, it lacks the appearance of methodical discipline. Detractors view this as a weakness.

Single-Point Failure Analysis (Ref. 10)

Method: Examine system, element by element. Identify those discrete elements and/or interfaces whose malfunction/failure, taken individually, would induce system failure.

Application: The technique is equally applicable to hardware systems, software systems, and formalized human operator procedures.

Thoroughness: Thoroughness by simple "inspection" methods is usually viewed as marginal or inadequate for systems having more than some arbitrarily small number of elements. When performed as an adjunct to another method (see Comments, below), thoroughness is then dictated by the depth to which that other, primary analysis is pursued.

Mastery Required: Mastery by simple "inspection" methods is readily found in the competent system analyst/designer. Mastery as an adjunct to other methods (see *Comments*, below) requires reasonable expertise at those other methods.

Difficulty of Application: Difficulty by "inspection" methods increases rapidly as system complexity (i.e., number of elements) increases. Difficulty when practiced as an adjunct to other methods (see *Comments*, below) generally requires little effort beyond that expended to practice those other methods.

Comments: Single-Point Failure Analysis is a natural consequence of the application of Fault-Tree Analysis, as used to determine cut sets. Single-Point Failure Analysis is also often accomplished through Event-Tree Analysis or Failure Modes and Effects Analysis.

Sneak-Circuit Analysis (Ref. 11, Section 5.5.1.2.c)

Method: Examine circuits (or command/control functions), searching out unintended paths (or control sequences) which – without component failure – can result in undesired operations, or in desired operations at inappropriate times, or which can inhibit desired operations.

Application: Sneak-Circuit Analysis is applicable to control and energy-delivery circuits of all kinds, whether electronic/electrical, pneumatic or hydraulic. Adaptations of the technique also see application in the analysis of software logic algorithms.

Thoroughness: The technique, when applied to a given system, tends to be exhaustively thorough at identifying all sneak paths of previously prescribed kinds. More problematical is the discovery of paths which lie outside previously prescribed classes.

Mastery Required: A basic understanding of control circuit theory is essential. Beyond that, little is required for analysis of uncomplicated systems. Several weeks of study and practice at application are necessary to develop mastery adequate for the analysis of more complex logic circuitry, however.

Difficulty of Application: Though quite time consuming, application is uncomplicated once mastery has been achieved. (Computer assisted methods are available.)

Comments: The technique enjoys a favorable reputation among control system designers who recognize it as a disciplined approach to the discovery of inadvertent design flaws.

Subsystem Hazard Analysis Ref. 1, pp 143-148)(Ref. 11, Section 5.5.1.2)

Method: Apply one or more hazard analysis techniques to system elements and components, or to arrays of them, at less-than-system level.

Application: To satisfy the definition, this form of analysis can be performed only upon subsystems – i.e., functionally discrete groupings of elements/components at less-than-system level. Beyond that restriction, application is universal.

Thoroughness: Thoroughness depends upon the technique(s) used and the depth to which they are employed. (See *Comments*, below.)

Mastery Required: Acquiring competence is dependent upon the technique(s) selected, with which to perform the Subsystem Hazard Analysis. (See *Comments*, below.)

Difficulty of Application: Selection of technique(s) to be used determines difficulty of application. (See *Comments*, below.)

---

*Often called "what if-ing" or "brainstorming"; cf., Maximum Credible Accident/Worst-Case Condition.

Comments: The Subsystem Hazard Analysis is not a discrete technique. Instead, it is the application of any technique, or any group of them, performed at less-than-system level.

System Hazard Analysis (Ref. 11, Section 5.5.1.3)

Method: Indistinguishable from Interface Analysis.

Application: Same as for Interface Analysis.

Thoroughness: Same as for Interface Analysis.

Mastery Required: Same as for Interface Analysis.

Difficulty of Application: Same as for Interface Analysis.

Systematic Inspection (Ref. 2, pp 16-19)(Ref. 7, pp 70-84)

Method: Using checklists, codes, regulations, industry consensus standards and guidelines, prior mishap experience and common sense, methodically examine a design/system/process, identifying discrepancies representing hazards.

Application: The technique is the single, most widely practiced of the many hazard discovery methods. Its application is virtually without limit.

Thoroughness: Thoroughness of application is determined by the degree to which codified checklists, etc. (see *Method*, above) are *available*, the degree to which those which are available are *applicable* to the system at hand, and the further degree to which they are actually *applied* in practice.

Mastery Required: Competent system designers will have developed the mastery required, simply as a result of having carried out the designs. Because a rote process is involved, mastery by others is easily achieved except for complex designs.

Difficulty of Application: Application involves, most often, a readily applied use of checklist data in a rote process.

Comments: Many system safety practitioners regard Systematic Inspection as an essential preliminary to the application of any other technique.

Comparison & Groupings

Certain of the hazard identification and analysis techniques summarized in this compendium are quite similar to others, both in concept and in application. Some have in common a reliance upon formalized logic methods. Others are best used, or can only be used, when aided by the practice of adjunct techniques. It is helpful to group the techniques according to such similarity features. Such groupings of the techniques aid in their selection and use, and in the interpretation of results obtained by them*:

Techniques Largely Reliant upon Others:
- Subsystem Hazard Analysis
- Single-Point Failure Analysis
- Contingency Analysis
- System Hazard Analysis
- Preliminary Hazard Analysis
- Interface Analysis
- Criticality Analysis

Techniques Largely Identical

Group I
- Procedure Analysis
- Job Safety Analysis
- Operating & Support Hazard Analysis

Group II
- Interface Analysis
- System Hazard Analysis

Group III
- Flow Analysis
- Energy Analysis

Techniques Based on Logic Methods:
- Event-Tree Analysis
- Management Oversight & Risk-Tree Analysis
- Failure Modes & Effects Analysis
- Network Logic Analysis
- Fault-Tree Analysis
- Sneak-Circuit Analysis

"What-If" Methods:
- Maximum Credible Accident/Worst-Case Condition
- Scenario
- Critical Incident Technique

Of the techniques presented in this compendium, not all lend themselves to inclusion in the groupings developed above. Those which defy such grouping are:

- Change Analysis
- Systematic Inspection
- Naked Man
- Prototype

References

1. Hammer, Willie; "Handbook of System and Product Safety"; Prentice-Hall, Inc.; 1972.
2. "Supervisors Safety Manual"; National Safety Council; 1976 (Fourth Edition)
3. "Systems Safety"; Notes for Course No. 529; The George Washington University; May 1979.
4. Briscoe, G.J.; "Risk Management Guide"; EG&G Idaho, Inc.; SSDC-11; June 1977.
5. Johnson, William G.; "MORT Safety Assurance Systems"; Marcel Dekker, Inc.; 1980.
6. Kije, L.T.; "Residual Risk"; Russe Press; 1963.
7. McElroy, F. (Editor); "Accident Prevention Manual for Industrial Operations"; National Safety Council; 1974 (Seventh Edition).
8. Hammer, Willie; "Occupational Safety Management and Engineering"; Prentice-Hall; 1981.
9. Hrzina, J.; "Single-Point Failure Analysis in System Safety Engineering"; *Professional Safety;* Vol. 25, No. 3, p 20, March 1980.
10. Kepner, Charles, H. and Tregoe, Benjamin B.; "The Rational Manager"; McGraw-Hill; 1965.
11. Anonymous; "System Safety Program Requirements"; MIL-STD-882A; 28 June 1980.
12. Bullock, M.G.; "Change Control and Analysis"; EG&G Idaho, Inc.; SSDC-21; March 1981.
13. Lewis, H.W.; "The Safety of Fission Reactors"; *Scientific American;* Vol. 242, No. 3, p 53, March 1980.
14. Vesely, W.E., et al; "Fault-Tree Handbook"; NUREG-0492; U.S. Government Printing Office; January 1981.

---

*Of the techniques presented in this compendium, some have multiple attributes and thus appear in more than one grouping.

APPENDIX E

SELECTED BIBLIOGRAPHY

TRANSPORTATION DEVELOPMENT CENTRE
TRANSPORTATION SYSTEMS SAFETY
SELECTED BIBLIOGRAPHY

1. GENERAL

Blake, Stewart P. Managing for responsive research and development. San Francisco: W.H. Freeman, 1978.

Canada. National Research Council. Scientific Policy, Research and Development. Bibliography prepared for the Canada Institute for Scientific and Technical Information. Ottawa, 1981.

Clarke, Thomas E. Decision-making in technologically-based organizations: a literature review of present practice. Ottawa: Ministry of State for Science and Technology, January 1974.

Clarke, Thomas E. R&D Management Bibliography 1981 (3rd Edition). Vancouver, B.C.: Stargate Consultants Limited, 1981.

Plott, C.R. A review of decision theoretic literature with implications regarding governmental research and development policies. Social Science Working Paper No. 49. California Institute of Technology, Pasadena, California, September 1974.

Roads and Transportation Association of Canada. Transportation R&D in Canada. Ottawa, Annual.

Summary of awards and published reports under the programs of university research for fiscal years 1973 and 1974. Washington, D.C.: United States. Dept. of Transportation, [1974 or 1975].

United States. General Services Administration. U.S. government manual 1982-1983. Washington, D.C.: Government Printing Office, 1982.

United States. Dept. of Transportation. Directory 1983. Washington, D.C.: Government Printing Office, 1983.

United States. National Aeronautics and Space Administration. Directory of Aerospace Safety Specialized Information Sources. Washington, D.C.: NTIS. Volume I, October 1973, Volume II, April 1976.

United States. Transportation Research Board. Highway Safety Literature. Quarterly publication. Washington, D.C.

Vance Bibliographies. *Transportation Accidents: A Guide to Published Statistical Sources*. Monticello, Illinois: Public Administration Series: Bibliography #P368, 1979.

2. R&D POLICY AND PLANNING

Bailey, Kay. "U.S. National Transportation Safety Board" in *Hazard Prevention*, (March-April, 1978), pp. 25-26.

Brown, David B. *Systems analysis and design for safety - safety systems engineering*. Englewood Cliffs, New Jersey: Prentice-Hall, 1976.

Canada. Dept. of Industry, Trade and Commerce. *Report to major project task force by transportation subcommittee*. Ottawa: Author, 1980.

Canada. Ministry of State for Science and Technology. *R&D policies; planning and programming*. Ottawa: Supply and Services, 1981.

Canada. Secretariat to the Panel on Transportation R&D. *Transportation research and development*. rev.ed. Ottawa: Author, 1978.

Canada. Transport Canada. *TDC annual report 1980-1981*. Montreal: Transportation Development Centre, 1981.

Canada. Transport Canada. *Towards a research and development policy for Transport Canada*. 2 vol. Ottawa: Supply and Services, 1982.

Chiogioji, M.H. *A critical analysis of federal R&D project selection methodology for water quality projects*. Ph.D. Dissertation. The George Washington University, Washington, D.C. 1972.

Costello, Denis. *A Practical Approach to R&D Project Selection*. Technological Forecasting and Social Change, August 1983.

Covello, Vincent T. *The Perception of Technological Risks: A Literature Review*. Technological Forecasting and Social Change, August 1983.

Glater, David S., and Maney, Accola. *Review of safety related statutory authority administered by the Department of Transportation - interim report, October 1973*. Washington, D.C.: United States. Dept. of Transportation, [1973?]. DOT-TSC-OST-73-45.

Gruver, James E.,...et al. Highway investment analysis package. [s.l.]: Committee on Application of Economic Analysis to Transportation Problems, [1976?].

Horodniceanu, Michael and Cantilli, Edmond J. Transportation system safety. Lexington, MA.: Lexington Books, 1979.

International Association of Traffic and Safety Sciences. Japanese government white paper on transportation safety - Prime Minister's Office, 1982. [Washington, D.C.?]: Author, 1982.

Juster, Richard D. an[illegible]cknold, Wayne M. Improving the process of programming transp[illegible]tion investments. [s.l.]: Committee on Application of Economic Analysis to Transportation Problems, [1975?].

Knox, Ronald R., Martin, Theodore K. and Yuskus, William J. Programming highway improvements in new funding environment. [s.l.]: Committee on Transportation, Planning, and Evaluation, [1976 or 1977].

Malasky, Sol. W. System safety: technology and application. 2nd Ed. New York: Garland STPM Press, 1982.

March, James G. Theories of choice and the making of decisions. Washington, D.C.: American Association for the Advancement of Science, 1982.

National Science Foundation. Instructions for annual survey of federal funds for research and development. Vol. XXXII. Washington, D.C.: Author, 1983.

National Transportation Safety Board. Annual report to Congress. Washington, D.C.: Government Printing Office, 1982.

Organisation for Economic Co-operation and Development (OECD). Analytical Methods in Government Science Policy: An Evaluation. Science Policy Studies. Paris, 1972.

Rand Corporation. R&D management: methods used by federal agencies. Santa Monica, California: January 1974.

"Report on joint conference Eno Foundation board of directors and board of consultants" in Traffic Quarterly, [1977?], pp. 173-262.

Salem, Steven L. and Kenneth, Soloman A. A preliminary survey of risks and safety operations at selected universities. Santa Monica, CA: Rand Corporation, 1982.

United States. Dept. of Transportation. Department of Transportation Safety Programs and Plans. Washington, D.C.: Author, 1968.

United States. Dept. of Transportation. Proceedings of the Department of Transportation Interdepartmental Safety Seminar, December 16-17, 1968. Washington, D.C.: NTIS PB182 288, January 1969.

United States. Dept. of Transportation. Analysis of fiscal year 1977 DOT program by policy and RD&D management objectives. Vol. I. Washington, D.C.: Author, 1976.

United States. Dept. of Transportation. Department of Transportation allocations for safety: FY 1973 estimated budget authority. Washington, D.C.: Government Printing Office, 1972.

United States. Dept. of Transportation. Guide to the DOT R&D management system. Washington, D.C.: Author, [197-?].

United States. Dept. of Transportation. 1984 budget; excerpts from the President's budget. Washington, D.C.: Government Printing Office, 1983.

United States. Dept. of Transportation. Problem identification manual for traffic safety programs; vols I & II. Washington, D.C.: Author, 1976.

United States. Dept. of Transportation. Profile of the 1980's. Washington, D.C.: Government Printing Office, 1980.

United States. Dept. of Transportation. Research and development policy statement of the Department of Transportation. Washington, D.C.: Government Printing Office, 1981.

United States. Office of Science and Technology Policy. Annual science and technology report to the Congress: 1981. Washington, D.C.: Government Printing Office, 1981.

Young, Fred. Final Report of the Select Committee on Highway Safety. Toronto: Queen's Printer, 1977.

3. SYSTEM SAFETY METHODOLOGY

Ad hoc Committee on Accident Data Collection. *Accident Data Availability*. Ottawa: Canada Safety Council, December 1978.

American Association for Automotive Medicine. Committee on Injury Scaling. *The abbreviated injury scale 1976 revision*. Morton Grove, IL: Author, 1976.

Ang, A.H.S.,...et al. *Development of a systems risk methodology for single and multi-modal transportation systems*. Urbana, IL: University of Illinois, 1979. Prepared for the U.S. Department of Transportation.
DOT-RSPA-DPB-50-79-16.
NTIS PB80-105539

Atzinger, E.M. and Brooks, W.J. *Compendium on risk analysis*; Special publication no. 4. Aberdeen, MD: Army Material Systems Analysis Agency, 1972.

Baker, Susan P. "Injury classification and the international classification of diseases codes" in *Accident Analysis and Prevention*, vol. 14; no. 3 (1982), pp. 199-201.

Benner, Ludwig. "Safety, risk and regulation; basic concepts for 'safety' risk analysis" in *Transportation Research Forum* [1972?], pp. 336-353.

Benner, Ludwig and McDewitt, Joyce A. "System safety methodology" in *Hazard Prevention*, (Sept.-Oct., 1982), pp. 14-16, 26-31.

Boyd, Don A. "The analysis of transportation risks from a shipper's viewpoint" in *Transportation Research Forum* [1971?], pp. 375-386.

Canada. Transport Canada. *State of the art review; risk analysis*. Ottawa: Author, 1981.

Canada Grains Council. *Current status of research needs relating to the capacity of the eastern grain handling and transportation system*. Winnipeg: Author, 1980.

Cantilli, E.J. *Transportation system safety*. New York: Polytechnic Institute of New York, [1968?].

Clark, E.M. and Van Horn, A.J. *Risk-benefit analysis and public policy: a bibliography*. Cambridge, MA: Harvard University Energy and Environmental Policy Center, 1976.

Clemens, P.L. "A compendium of hazard identification and evaluation techniques for system safety application" in Hazard Prevention, (March-April, 1982), pp. 11-18.

The Conference Board. Toward a reconstruction of federal budgeting. New York: Author, 1983.

Gardenier, John S. "A search for a practical spill risk model" in Transportation Research Forum, (June, 1972), pp. 355-364.

Garrison, W.L., Thomas, E.N., and Worrall, R.D. Data system requirements for urban and regional models. Evanston, IL: Northwestern University, 1976.

Geffen, C.A. and Andrews, W.B. Risk; a measure of transportation system safety. San Diago, CA: s.n., 1970.

Graham, Kenneth J. and Kinney, Gilbert F. "A practical safety analysis system for hazards control" in Journal of Safety Research, vol. 12; No. 1, (Spring, 1980), pp. 13-20.

Haddon, William Jr. "The basic strategies for reducing damage from hazards of all kinds" in Hazard Prevention, (September-October, 1980), pp. 8-12.

Hauer, Ezra. Evaluation research in transportation safety - the Bayesian alternative. Toronto: University of Toronto, May 1981.

Hollenback, John J. Jr. Failure mode and effect analysis. Milwaukee: Allis-Chalmers Corporation, 1977. Prepared for the Society of Automotive Engineers, Inc.

Horodniceanu, M. and Cantilli, E.J. Transportation system safety methodology. New York: Polytechnic Institute of New York, 1976. Prepared for the U.S. Department of Transportation, Office of University Research. DOT-TST-77-17. NTIS PB262 793

Horodniceanu, M.,...et al. System safety techniques useful for transportation safety. New York: Polytechnic Institute of New York, 1977.

Intendes Group Limited. Pilot research study of transportation safety. Toronto: Author, 1972.

Johnson, William G. "Mort: The management oversight and risk tree" in journal of safety resarch, vol. 7; no. 1 (March, 1975), pp. 4-20.

Kastenburg, W.E.,...et al. On risk assessment in the absence of complete data. Los Angeles: U.C.L.A. School of Engineering and Applied Sciences, July 1976.
NTIS PB261 573.

McGuire, Charles W. "Risk analysis for transportation safety; the regulator's viewpoint" in Transportation Research Forum, [1972?], pp. 393-399.

Miller, C.O. Development and description of system safety. Adelphi, MD: American Society of Safety Engineers, 1969.

Moriarty, Brian. "Life cycle cost of safety estimation" in Hazard Prevention, (March-April, 1978), pp. 16-21.

Okrent, D., ed. Risk-benefit methodology and applications: some papers presented at the Engineering Foundation Workshop. Los Angeles, CA: University of California School of Engineering and Applied Science, 1975.

Peters, George A. "Why only a fool risks on safety standards" in Hazard Prevention, (November-December, 1977), pp. 12-14.

Philipson, Lloyd L. Investigation of the feasibility of the Delphi technique for estimating risk analysis parameters; final report. Los Angeles, CA: University of Southern California, 1974.

Prensky, S.,...et al. The status of transportation safety. Cambridge, MA.: United States. Dept. of Transportation, 1982.

Raheja, Div. "Systems safety: Concepts and applications" in Hazard Prevention, (March-April, 1980), pp. 20-21.

Road and Transportation Association of Canada. Guide to evaluation of safety programs. Ottawa: Author, 1981.

Sabey, Barbara E. and Taylor, Harold. "The known risks we run: the highway" in Societal risk assessment. Edited by Richard C. Schwing and Walter A. Albers. New York: Plenum Press, 1980. pp. 43-70.

Starr, C., Rudman, R. and Whipple, C. "Philosophical basis for risk analysis" in Annual Review of Energy, Vol. 1 (1976), p. 629.

"The state of the art of system safety" in Hazard Prevention, (May-June, 1982), pp. 17-31.

Surry, Jean. Industrial accident research: A human engineering appraisal. Toronto: Ontario Government Publications Service, 1979.

"System safety management; The new DOD program requirements" in Hazard Prevention, (September-October, 1977), pp. 11-17.

Transportation Research Board. Transportation system safety and project analysis. Washington, D.C.: Author, 1979.

United States. Dept. of Transportation. Research and development activities in the department of transportation and selected federal agencies. Washington, D.C.: Government Printing Office, 1980.
NTIS PB81-132888

United States. Dept. of Transportation. Transportation systems safety methodology. Washington, D.C.: Government Printing Office, 1976.

United States, Dept. of Transportation. Emerging transportation planning methods. Washington, D.C.: Government Printing Office, 1978.
NTIS PB81-119133

United States. World Health Organization. Home accidents - A European strategy for prevention. Geneva: Author, 1982.

Yerrell, J. Stuart, ed. Transport research for social and economic progress; proceedings of the World Conference on Transport Research. London, Eng.: Gower Press, 1980.

4. AIR

Andrews, Frank G. "Aircraft accident investigation" in Hazard Prevention, (March-April, 1980), pp. 22-24.

Batelle Columbus Laboratories. Evaluation of safety programs with respect to the causes of air carrier accidents. Columbus: Author, 1980. Report No. ASP80-1.

Batelle Columbus Laboratories. Evaluation of safety programs with respect to the causes of general aviation accidents. 2 vols. Columbus: Author, 1980.

Batelle Columbus Laboratories. *Evaluation of safety programs with respect to the causes of general aviation accidents*. 2 vols. Columbus: Author, 1980.

Canada. Transport Canada. *The intercity for-hire trucking of dangerous goods in Canada*. Ottawa: Author, 1982.

Canada. Transport Canada. *The transport of dangerous goods by rail in Canada*. Ottawa, Author, 1982.

Civil aviation research and development policy study; report. Washington, D.C.: U.S. Dept. of Transportation/NASA, 1971.

Dieterly, Duncan L. "Decision/problem analysis in aircraft accident reconstruction" in *Journal of Safety Research*, vol. 11; no. 4 (Winter, 1979), pp. 146-155.

"The economics of safety" in *Flight International*, (August 28, 1975), pp. 281+

"FAA's budget underscored by aviation safety" in *Aviation Week and Space Technology*, (February 7, 1977), pp. 56-57.

Fritsch, Olof. "Some thoughts on aircraft accidents and their prevention" in *ICAO Bulletin*, (September 1976), pp. 24-27.

Fullerton, Eleanor & Linda S. Rubens. *Directory of aerospace safety specialized information sources*. Falls Church, Virginia: National Aeronautics and Space Administration, 1983. NASA-CR121206.

Hodge, Kenneth E. "Research developments for aircraft safety" in *Aircraft Engineering*, (January, 1980), pp. 10-15.

International Civil Aviation Organization. *International standards and recommended practices*. Montreal: Author, 1981.

International Civil Aviation Organization. *Accident prevention manual*. Montreal: Author, 1982.

Lederer, J., Miller, C.O. and Schmidt, C.F. Economics of safety in civil aviation. New York: Flight City Foundation, 1963. Prepared for the Federal Aviation Agency.

Lederer, Jerome. "The economic and social impact of aerospace safety" in ICAO Bulletin, (September, 1976), pp. 30-34.

Miller, C.O. State of the art in air safety; proceedings of the Symposium on Air Safety. Dallas: Southern Methodist University, 1968.

Noah, J.W.,...et al. Cost benefit analysis and the national aviation system; a guide. Falls Church, VA: J. Watson Noah Associates, 1977. Prepared for United States. Dept. of Transportation. Report No.: FAA-AVP-77-15.

Peat, Marwick et Associés. The costs of aircraft accidents in Canada. Montreal: Author, 1981.

Peters, George A. "How to design a safe aircraft" in Hazard Prevention, (March-April, 1979), pp. 6-11.

Rallis, Tom. Intercity transport engineering and planning. Copenhagen: Technical University of Denmark, 1979.

Society of Automotive Engineers. U.S. general aviation safety record. Wichita: Author, 1971.

United States. General Accounting Office. Report by the Comptroller General of the United States: How to improve the Federal Aviation Administration's ability to deal with safety hazards. Washington, D.C.: U.S. General Accounting Office, February 29, 1980. Report CED-80-66.

United States. Congress. Office of Technology Assessment. Review of the FAA 1982 national airspace system plan. Washington, D.C.: Government Printing Office, 1982.

United States. Congress. Subcommittee on Transportation, Aviation and Materials. Aviation safety research. Washington, D.C.: Government Printing Office, 1982.

United States. Congress. Hearings before the Subcommittee on Aviation of the Commitee on Public Works and Transportation. Washington, D.C.: Government Printing Office, 1980.

United States. Dept. of Transportation. Federal Aviation Agency. The National Airspace System (NAS) plan for engineering and development. (Unpublished preliminary draft, January, 1983).

United States. Dept. of Transportation. Federal Aviation Administration. Office of Aviation Safety. What is ASAS? (Aviation Safety Analysis System) Washington, D.C.: Government Printing Office, 1982.

5. MARINE AND HAZARDOUS MATERIALS

Arthur D. Little. A modal economic and safety analysis of the transportation of hazardous substances in bulk; final report. Washigton, D.C.: U.S. Dept. of Commerce, Marine Administration, [197-].

Bierlein, Lawrence W. Hazardous materials: a guide for state and local officials. Washington, D.C.: U.S. Dept. of Transportation, 1982.

Canada. Cabinet Committee on Foreign and Defence Policy. Report on an evaluation of search and rescue. Ottawa: Supply and Services, 1982.

Canada. Dept. of Communications. "Use of satellites for search and rescue, tested in Canada" in I.C.A.O. Bulletin, (September, 1976).

Canada. Transport Canada. Coast Guard. Code of recommended standards for the prevention of pollution in marine terminal systems. Ottawa: Supply and Services, 1977.

Cheaney, E.S., Leis, R.D. and Coyle, A.J. RDT&E plan for marine safety. Columbus, Ohio: Batelle Columbus Laboratories, 1977. Prepared for the United States Department of Transportation

Cook, R.C., Marino, K.L. and Cooper, R.B. A simulator study of deepwater port shiphandling and navigation problems in poor visibility; final report. Washington, D.C.: U.S. Dept. of Transportation, 1981.
NTIS AD A100-656

Commercial vessel safety; economic benefits; Appendix A - Estimation procedures for benefits of marine safety regulations; final report. Washington, D.C.: U.S. Dept. of Transportation, 1980. NTIS A098-312

Dunn, W.A. and Tullier, P.M. Spill risk analysis program, phase II: Methodology development and demonstration; Final report part I. Springfield, VA: National Technical Information Service, 1975.

Faragher, W.E.,...et al. Deepwater ports approach/exit hazard and risk assessment; final report. Washington, D.C.: U.S. Dept. of Transportation, 1979. NTIS AD A074-529

Gabor, Tim and Griffith, Terrik. The assessment of community vulnerability to acute hazardous materials incidents. Columbus, Ohio: Ohio State University Disaster Research Center, 1979.

Gardenier, John S. Toward a science of marine safety. The Hague: Symposium on Marine Traffic Systems, 1976.

Gardenier, John S...et al. Risk management for Coast Guard regulatory decision-making. Washington, D.C.: Dept. of Transportation, 1975.

Gardenier, J.S. and Stoehr, L.A. Collision region; A new mathematical concept for safe navigation. The Hague: Fourth Ship Control Systems Symposium, 1977.

Jones, George P.,...et al. Risk analysis in hazardous materials transportation; vol. 1: final report. Los Angeles, CA: University of Southern California, 1973.

Jones, George P. and Barrow, R.W. Risk analysis in hazardous materials transportation; vol. 2: bibliography. Los Angeles, CA: University of Southern California, 1973.

Luckritz, Robert T., and Schneider, Alan L. Decision-making in hazardous materials transportation. In presented papers to the Fifth International Symposium on the Transport of Dangerous Goods by Sea and Inland Waterways, Vol. II, Hamburg, April 1978.

Lynch, Cornelius, J., Eisenberg, Norman A. and Maton, John D. Vulnerability model for marine spills harzardous materials. Rockville, MD: Enviro Control, 1975.

Murphy-Wong, Sandra. Guide to marine transportation information sources in Canada - Phases I and II. Montreal: Transport Development Centre, 1980.

Murphy-Wong, Sandra. Listing of Canadian marine R&D projects 1980. Montreal: Transport Development Centre, 1980.

Paramone, B.,...et al. Human and physical factors affecting collisions, rammings, and groundings on western rivers and gulf intracoastal waterways. Washington, D.C.: U.S. Dept. of Transportation, 1979. NTIS AD A074-290

Paramone, B.,...et al. Study of task performance problems in reports of collisions, rammings, and groundings in harbors and entrances; final report. Washington, D.C.: U.S. Dept. of Transportation, 1979. NTIS AD A071-058

Perry, Willard W., and Articola, William P. Study to modify the vulnerability model of the risk managment system; final report. Washington, D.C.: U.S. Dept. of Transportation, 1980. NTIS AD A084-214

Raj, Phani P.K. and O'Farrel, Peter M. Development of additional hazard assessment models. Washington, D.C.: Dept. of Transportation, 1977.

Russell, E.R.,...et al. A community model for handling hazardous materials transportation emergencies. Washington, D.C.: U.S. Dept. of Transportation, 1981.

Russell, E.R.,...et al. Risk assessment users manual for small communities and rural areas. Washington, D.C.: U.S. Dept. of Transportation, 1981.

Russell, E.R.,...et al. Risk assessment/vulnerability users manual for small communicaties and rural areas. Washington, D.C.: United States. Dept. of Transportation, 1981.

Russell, E.R.,...et al. A community model for handling hazardous material transportation emergencies. Washington, D.C.: United States. Dept. of Transportation, 1980.

Safety in shipping; A Seatrade study. London, Eng.: Seatrade Publications, 1976.

Simons, John A. and Erdman, Robert C. Risk assessment strategy for marine transportation. Washington, D.C.: Dept. of Transportation, 1975.

Stoehr, Leonard A.,...et al. Spill risk analysis, phase II: methodology development and demonstration; Final report, part II, volume I. Springfield, VA: NTIS, 1975.

Tihansky, Dennis P. A conceptual framework for risk-benefit assessment of hazardous materials transport. Washington, D.C.: Dept. of Transportation, 1975.

Transport Canada. Canadian Coast Guard. Casualty Investigations. Marine Casualty Information System Reports. Ottawa, Annual.

Transport Canada. Transport Dangerous Goods. Dangerous Goods Occurrence Reports. Ottawa. Annual.

Transportation Research Board. The ten most critical issues in hazardous materials transportation; Transportation research circular. Washington, D.C.: National Academy of Sciences, 1980.

Uh, Ihn H. Risk analysis of dangerous commodity transportation: a survey of theories, methodologies and empirical studies. Ottawa: Canadian Transport Commission, 1982.

United States. Dept. of Transportation. Coast Guard roles and missions. Washington, D.C.: Government Printing Office, 1982.

United States. Dept. of Transportation. Hazardous materials; 1980 emergency response guidebook. Washington, D.C.: Author, 1980.

United States. Dept. of Transportation. Hazardous materials - A guide for state and local officials. Washington, D.C.: Author, 1982.

United States. Dept. of Transportation. Coast Guard. *Activities relating to Title II Ports and Waterways Safety Act of 1972*. Washington, D.C.: Author, [19--].
NTIS AD A057-607

United States. Dept. of Transportation. Coast Guard. *Analysis of risk in the water transportation of hazardous materials*. Washington, D.C.: Author, [19--].
NTIS AD A023-505

United States. Dept. of Transportation. Coast Guard. *Assessment models in support of the hazard assessment handbook*. Washington, D.C.: Author, [19--].
NTIS AD 775-756

United States. Dept. of Transportation. Coast Guard. *CHRIS: a condensed guide to chemical hazards*. Washington, D.C.: Author, [19--].
NTIS AD A001-242

United States. Dept. of Transportation. Coast Guard. *Commercial vessel safety risk assessment study*. Vol. I; *Survey of data for marine risk assessment*. Washington, D.C.: Author, [19--].
NTIS AD A077-328

United States. Dept. of Transportation. Coast Guard. *Commercial vessel safety risk assessment study*. Vol. II; *Risk assessment methodology survey*. Washington, D.C.: Author, [19--].
NTIS AD A076-437

United States. Dept. of Transportation. Coast Guard. *A critical technical review of six hazard assessment models*. Washington, D.C.: Author, [19--]
NTIS AD A00-242

United States. Dept. of Transportation. Coast Guard. *Cost, benefit and effectiveness of the merchant marine safety program*. Washington, D.C.: Government Printing Office, 1968.

United States. Dept. of Transportation. Coast Guard. *A critical technical review of six additional hazard assessment models*. Washington, D.C.: Author, [19--].
NTIS AD A047-342

United States. Dept. of Transportation. Coast Guard. *Regulatory effectiveness methodology; Phase I: research*. Washington, D.C.: Author, [19--].
NTIS AD 785-026

United States. Dept. of Transportation. Coast Guard. Regulatory effectiveness methodology; Phase II; research. Washington, D.C.: Author, [19--].
NTIS AD A071-056

United States. Dept. of Transportation. Coast Guard. Risk analysis methods for deepwater port oil transfer systems. Washington, D.C.: Author, [19--].
NTIS AD A025-298

United States. Dept. of Transportation. Coast Guard. Spill risk analysis program; Phase II: methodology development and demonstration. Washington, D.C.: Author, [19--].
NTIS AD 785-026

United States. Dept. of Transportation. Coast Guard. A study of cost, benefits and effectiveness of the Merchant Marine Safety Program. Washington, D.C.: Author, [19--].
NTIS AD 777-025

United States. Dept. of Transportation. Coast Guard. Third-stage development of the vulnerability model; a simulation system for assessing damage resulting from marine spills. Washington, D.C.: Author, [19--].
NTIS AD A018-722

United States. Dept. of Transportation. Coast Guard. Vessel safety model. Vol. I; Analytic development. Washington, D.C.: Author, [19--].
NTIS AD A029-329 and AD 770-712

United States. Dept. of Transportation. Coast Guard. Vessel safety model. Vol. II; User's manual. Washington, D.C.: Author, [19--].
NTIS AD 772-726

United States. Dept. of Transportation. Coast Guard. Vessel safety model. Vol. III; Programmers' manual. Washington, D.C.: Author, [19--].
NTIS AD 773-586

United States. Dept. of Transportation. Coast Guard. Vulnerability model; a simulation system for assessing damage resulting from marine spills. Washington, D.C.: Author, [19--].
NTIS AD A015-171

United States. Dept. of Transportation. Materials Transportation Bureau. Toward a federal/state/local partnership in hazardous materials transportation safety. Washington, D.C.: Author, 1982.

United States. Dept. of Transportation. Research Programs Administration. Office of Regulatory Planning and Analysis. The study of the capability of risk analysis for the support of the formulation of regulations for the transportation of hazardous materials. Los Angeles, CA: University of Southern California, [19--].

United States. National Research Council. A review of the Department of Transportation Research and Special Programs Administration's hazardous materials research and development program. Washington, D.C.: Government Printing Office, 1980.
NTIS PB83-138099

United States. Office of Management Planning. Report of the Hazardous Materials Transportation Task Force. Washington, D.C.: Hazardous Materials Task Force, 1978. DOT-RSPA-78-2.

Urbanek, G. and Barber, E. (Peat, Marwick, Mitchell & Co.) Development of criteria to designate routes for transporting hazardous materials. Springfield, VA: NTIS; 1980.

Ware, J.R., Best, J.F., and Curry, R.E. Modeling human behaviour for marine safety investigations. Report prepared by Operations Research Inc. for the Dept. of Transportation. Coast Guard. Washington, D.C. March 1980.
NTIS AD A084-184

Williams, Kerry N. and Sheldon, Dan. A risk assessment methodology for the highway transportation of hazardous materials. Santa Monica, CA: Economath Systems, 1980.

Wheatley, Stanley D. Simulation technology and traffic accident records systems. New York: National Maritime Research Center, 1979. Prepared for the Transportation Research Board, Commission on Sociotechnical Systems, National Research Council.

Zajic, J.E. and Himmelman, W.A. Highway hazardous materials spills and emergency planning. New York: Marcel Dekker, 1978.

6. MASS TRANSIT AND RAIL

Canadian National Railway Company v. Ernest Norman, (1982) Supreme Court of Newfoundland, Court of Appeal.

Canadian National Railway. Safety backgrounder 1974-1980. Montreal: Author, 1981.

Canadian Transport Commission. Summary of Accidents - Incidents Reported to the Canadian Transport Commission. Ottawa, Annual.

Canadian Pacific Railway. Safety and accident prevention code. Montreal: Author, 1983.

Cheaney, E.S.,...et al. Safety in urban mass transportation: Guidelines manual. Columbus: Batelle Columbus Laboratories, 1975. Prepared for the U.S. Department of Transportation, Urban Mass Transit Administration, UMTA-RI-06-0005-75-2.

Cheaney, E.S.,...et al. Safety in urban mass transportation: Research report. Columbus: Batelle Columbus Laboratories, 1975. Prepared for the U.S. Department of Transportation, Urban Mass Transit Administration, UMTA-RI-06-0005-75-3.

Daley, D.M. and Leonard, E.T. Rail transit safety 1981 annual report. Cambridge, MA: U.S. Department of Transportation, 1982. Prepared for the U.S. Department of Transportation. UMTA-MA-06-0060-82-1.

J.C. Cooper et Associés. Part U.F. safety. Montreal: Author, [198-?] (Questionnaire on safety in Canadian railways)

Jones, G.P.,...et al. Development of a safety program plan for the Office of Safety and Product Qualification. Los Angeles: Institute of Safety and Systems Management, University of Southern California, 1977. Prepared for the U.S. Department of Transportation, Urban Mass Transportation Administration.
NTIS PB 279-331/332

Railway safety assessment; preliminary draft: Task I: Analysis of current and historical railroad accident/incident data; Task II: Analysis of government, industry and union railroad safety programs; Task V: Analysis of governmental and industry safety expenditures. Prepared by Peat, Marwick, Mitchell & Co. in association with R.L. Banks & Associates, Inc., Thomas K. Dyer, Inc. and Gibbs & Hill, Inc. for the U.S. office of Technology Assessment. Washington, D.C.: 1977.

United States. Congress. Office of Technology Assessment. An evaluation of railroad safety. Washington, D.C.: Government Printing Office, 1978. Report No. OTA-T-61

United States. Congress. Office of Technology Assessment. Impact of advanced group rapid transit technology. Washington, D.C.: Government Printing Office, 1980.

United States. Dept. of Transportation. *Plan for improving the management of railroad safety programs; A report to the U.S. Congress*. Washington, D.C.: Government Printing Office, 1981.

Zallinger, D.A., Rogers, B.A. and Johri, H.P. *Calculation of hazard indices for highway-railway crossings in Canada*. Ottawa: Department of Supply and Services, 1977.

Zobrak, Marcel J. *Track rehabilitation and maintenance research requirements*. McLean, VA: MITRE Corp, 1980. Prepared for United States. Dept. of Transportation. Report No. FRA/OR+D-80/09.

7. MOTOR CARRIER

Fleischer, G.A. *Simulation technology and traffic accident records systems*. Washington, D.C.: Transportation Research Board, 1979.

Transportation Research Board. "Truck accidents data systems: State of the art report" in *Transportation Research Circular*, No. 231 (September, 1981), pp. 1-8.

8. ROADS

American National Standards Institute. *Manual of classification of motor vehicle traffic accidents*. New York: Author, 1976.

American National Standards Institute. *Data element dictionary for traffic records systems: states' model motorist data base*. New York: Author, 1979.

Anderson, Thomas C. *Funding for highway safety research, development and demonstration in the National Highway Traffic Safety Administration*. Ann Arbor, Mich.: Highway Safety Research Institute, 1979. Prepared for the Motor Vehicule Manufacturers Association.

Arthur D. Little. *The state of the art of traffic safety*. New York: Praeger Publishers, 1972. Prepared for the Automobile Manufacturers Association, Inc.

Avishai, Ceder. "Traffic system safety-drivers' behavior, traffic flow, and road safety studies" in *Hazard Prevention*, (September-October, 1978), pp. 24-27.

Baker, R.F. The highway risk problem: policy issues in highway safety. New York: [s.n.], 1971.

Binder, Robert Henri. "Cost effectiveness in highway safety" in Traffic Engineering, (December, 1976), pp. 26-30.

Booz, Allen Applied Research. Vehicule-in-use safety analysis, Washington, D.C.: Government Printing Office, 1973. Prepared for the U.S. Department of Transportation.

Bowman, Mark A. A uniform transit safety records system for the Commonwealth of Virginia. Charlottesville, VA: Virginia Highway & Transportation Research Council, 1981.

Braun, Ronald R. and Roddin, Marc F. Quantifying the benefits of separating pedestrians and vehicles. Menlo Park, CA: Stanford Research Institute, 1978. Prepared for the American Association of State Highways and the Federal Highway Administration.

Brown, D.B. RAPID records analysis for problem identification and definition. Huntsville: Alabama Office of Highway and Traffic Safety, February 1980. Report 300-78-002-401-095.

Brühning, Ekkehard and Völker, Rolf. "Accident risk in road traffic - characteristic quantities and their statistical treatment" in Accident Analysis and Prevention, vol. 14; no. 1 (1982), pp. 65-80.

Canada. Transport Canada. An examination of motor vehicle accident modelling; final report prepared for the Road and Motor Vehicle Traffic Safety Branch. Ottawa: Supply and Services, 1977.

Canada. Transport Canada. Road and Motor Vehicle Traffic Safety Branch. Annual report 1981. Ottawa: Supply and Services, 1982.

Cantilli, E.J., Horodniceanu, M., and Pignataro, L.J. "System safety: a new approach to traffic safety" in Traffic Engineering, (December, 1976), pp. 36-38.

Chapman, A.J., Wade, F.M. and Foot, H.C. Pedestrian accidents. Chichester, Eng.: [s.n.], 1982.

Cleven, A.M. and Fucigna, J.T. The evaluation of highway traffic and safety programs: course guide. Darien, Conn.: Dunlop and Associates, 1976. Prepared for the U.S. Department of Transportation.

Cohen, J. and Preston, B. Causes and prevention of road accidents. London, Eng.: [s.n.], 1968.

Fonds d'Étude pour la Sécurité Routière. Sécurité routière: structures existantes en Belgique. Bruxelles: Author, [197-?].

Foot, H.C., Chapman, A.J. and Wade, F.M. Road Safety: research and practice. New York, Praeger, 1981.

Fortenberry, Jessie C. and Brown, David B. "Problem identification, implementation and evaluation of a pedestrian safety program" in Accident Analysis and Prevention, vol. 14; no. 4 (1982), pp. 315-322.

International Association of Traffic and Safety Sciences. IATSS research; Vol. 4. [s.l.]: Author, 1980.

International Road Federation. 1982 world survey of current research and development on roads and road transport. Washington, D.C.: Author, 1982. (Prepared for the U.S. Department of Transportation)

Joscelyn, K.B. and Jones, R.K. "Management of the traffic crash risk: a conceptual framework" in Journal of Safety Research, vol. 10; no. 4 (winter, 1978), pp. 148-161.

Laughland, J.C.,...et al. Methods for evaluating highway safety improvements; National cooperative highway research program report 162. Washington, D.C.: Transportation Research Branch, 1975.

Lawson, J.J. The costs of road accidents and their application in economic evaluation of safety programmes. Ottawa: s.n., 1978.

Lawson, J.J. "Canadian Department of Transport national driving survey 1978-1979" in Accident Analysis and Prevention, vol. 14; no. 5 (1982), pp. 371-380.

Lenz, D. Statement of the OECD Group S1: Major trends, approaches and overall concepts in the Federal Republic of Germany with respect to integrated safety programs. Paris: OECD, 1982.

Mateyka, J.A., Danzeisen, R. and Weiss, D.W. Faulttree applications to the automobile industry. Detroit: Society of Automotive Engineers, 1973.

Mateyka, J.A. and Talley, J. "System safety-risk analysis techniques applied to motor vehicles and rapid transit systems" in Journal of Safety Research, March 1977, vol. 9, no. 1, pp. 3-14.

Mayhew, M.A. The quality of national traffic accident statistics in Canada. Ottawa: Traffic Injury Research Foundation, 1981.

"Motor vehicle safety" in Role of the automobile study; Working paper no. 27. Ottawa: Supply and Services, 1979.

National Highway Traffic Safety Administration. Problem identification manual for traffic safety programs. Vols. I and II. Washington, D.C.: U.S. Dept. of Transportation, 1976.

Neilson, I.D. The theorical reconstruction of events leading to an impact in a road accident. Washington, D.C.: Dept. of the Environment, 1973.

Olsson, G.R., Mateyka, J.A. and Innes, J.J. Brake system safety analysis. Montreal: Society of Automotive Engineers, 1973.

Peat, Marwick, Mitchell & Co. Development of criteria to designate routes for transporting hazardous materials. Washington, D.C.: January 1980. Published by National Technical Information Service, Springfield, VA.

Peet, Richard C. "The year of evaluation" in Traffic Engineering, (December, 1976), pp. 31-35.

Roy Jorgensen Associates. Cost and safety effectiveness of highway design elements. Gaithersburg, MD: American Association of State Highway, 1978.

Simpson, H.M. and Warren, R.A. Utility and feasibility of merging secondary data sources in the study of road crashes. Ottawa: Traffic Injury Research Foundation, [19--].

Simpson, H.M. Data needs in the study of road crashes: persisting and emerging issues. Ottawa: Traffic Injury Research Foundation, 1982. Paper presented as part of the Conference on the Statistical Implications of Emerging Health Issues and Outlooks.

Simpson, H.M. The role of alcohol in traffic crashes: how good are the data? Ottawa: Traffic Injury Research Foundation of Canada, 1978. Invited address to the International Medical Advisory Conference.

Simpson, H.M., Pagé-Valin, L. and Warren, R.A. "A data base on traffic fatalities" in Journal of the Canadian Society of Forensic Sciences, vol. II; no. 3 (1978), pp. 215-219.

Sivak, Michael. Human factors and highway accident causation: some theorical considerations. Ann Arbor, Michigan: Highway Safety Research Institute, 1980.

Society of Automotive Engineers. Crash protection SP-J13; Proceedings of the International Congress and Exhibition. Detroit: Author, 1982.

Sorés Inc. Survey of Canadian traffic accident information systems; summary. Montreal, Quebec: Transport Canada, 1971.

Tarrants, William E. and Voas, Robert B. Highway safety needs study; 1981 update of 1976 report to Congress. Washington, D.C.: U.S. Dept. of Transportation, 1981.
PB83-158584

Transportation Research Board. Traffic accident analysis. Washington, D.C.: Author, 1974. Four Reports prepared for the 53rd Annual Meeting of the Highway Research Board.

Transportation Research Board. Traffic accident analysis and application of systems safety. Washington, D.C.: Author, 1980.

Transportation Research Board. Future of the national highway safety program. Washington, D.C.: National Academy of Sciences, 1977. Proceedings of a conference held March 6-9, 1977, in Warrenton, Virginia.

Transportation Research Board. Transportation system safety and project analysis. Washington, D.C.: National Academy of Sciences, 1979.

United States. Congress. Committee on Interstate and Foreign Commerce. Research needs in traffic safety. Washington, D.C.: Government Printing Office, 1958.

United States. Congress. Office of Technology Assessment. Automobile transportation system; summary and findings. Washington, D.C.: Government Printing Office, 1979.

United States. Congress. The status of the nation's highways: conditions and performance. Washington, D.C.: Government Printing Office, 1977.

United States. Dept. of Transportation. National Highway Traffic Safety Administration. Planning for safety priorities; 1983 safety priorities plan. Washington, D.C.: Author, 1983.

United States. Dept. of Transportation. Proceedings of the International Conference on Vehicle and Highway Safety. Washington, D.C.: Author, 1971.

United States. Dept. of Transportation. Statement for the OECD road transport research group on concept and methodologies for integrated safety programs. Washington, D.C.: Author, 1983.

United States. Dept. of Transportation. National Highway Traffic Safety Administration. An assessment of the Adequacy of NHTSA's Motor Vehicle Safety Research Plan, Findings of a Workshop. Washington, D.C.: Author, June 1979.
NTIS PB80-203680

United States. Dept. of Transportation. National Highway Traffic Safety Administration. Motor vehicle safety 1980. Washington, D.C.: Government Printing Office, 1980.

United States. Dept. of Transportation. National Highway Traffic Safety Administration. Highway safety 1980. Washington, D.C.: Government Printing Office, 1980.

United States. Dept. of Transportation. National Highway Traffic Safety Administration. Workshop to Review Problem-Behaviour Research Programs: Pedestrian, Bicycle and Pupil Transportation Safety. Washington, D.C.: Author, Sept. 1981
NTIS PB82-183658 (see also PB81-220725)

United States. Department of Transportation. National Highway Safety Needs Report. Report of the Secretary of Transportation to the United States Congress pursuant to Section 225 of the Highway Safety Act of 1973. Washington, D.C.: Government Printing Office, April 1976.

United States. Dept. of Transportation. National Highway Traffic Safety Administration. Traffic Accident Analysis and Application of Systems Safety. Washington, D.C.: Author, 1981.
NTIS PB81-103210

United States. Dept. of Transportation. National Highway Traffic Safety Administration. The economic cost to society of motor vehicle accidents. Washington, D.C.: Government Printing Office, 1983. DOT-HS-806-342

United States. Dept. of Transportation. National Highway Traffic Safety Administration. The automobile safety belt fact book. Washington, D.C.: Government Printing Office, 1977.

United States. Dept. of Transportation. National Highway Traffic Safety Administration. Funding for Highway Safety Research, Development and Demonstration in the NHTSA. Washington, D.C.: Author, 1980.
NTIS PB80-137672

Utah. Dept. of Transportation. FHWA safety file linkage demonstration project; system requirements definition, Salt Lake City: Author, 1983.

Visser, Evert J., ed. Transport decisions in an age of uncertainties; proceedings of the Third World Conference on Transport Research. Rotterdam: Martinus Mijhoff, 1977.

Voas, Robert E. and Tarrants, William E. Effectiveness and efficiencies in traffic safety programs - overview. Washington, D.C.: United States. Dept. of Transportation, 1982. Report no. DOT-HS-806-130.

Warren, R.A. "Research strategies in the study of fatalities" in Journal of the Canadian Society of Forensic Sciences, vol. 11; no. 4 (1978), pp. 275-281.

Warren, R.A. Treatment of missing data in road safety investigations: methodological innovations. Ottawa: Traffic Injury Research Foundation, 1980. Paper presented at the 17th Annual Meeting of the Traffic Injury Research Foundation of Canada.

Wilde, G.J.S. General survey of efficiency and effectiveness of road safety campaigns: achievements and challenges. The Hague: Dutch Road Safety Association, 1972.

Wilde, G.J.S. A critical view of countermeasure development and evaluation; proceedings. Stockholm: International Conference on Alcohol, Drugs and Traffic Safety, 1980.

Wilde, G.J.S., O'Neil, B. and Cannon, D. A psychometric investigation of drivers' concern for road safety and their opinions of various measures for accident prevention. Kingston, Ont.: Queen's University, 1975.

Wilde, G.S. and Murdoch, P.A. "Incentive systems for accident-free and violation-free driving in the general population" in Ergonomics, vol. 25; no. 10 (1982), pp. 887-888.

Williams, M.J. Validity of the traffic conflicts technique. Victoria, Australia: Australian Research Board, 1980.

Yerrell, J. Stuart, ed. Transport research for social and economic progress; Proceedings of the World Conference on Transport Research. Londong, Eng.: Gower Press, 1980. Vol. 4

Library and Information Centre / Centre de Documentation (GSLA)
RECEIVED - REÇU LE
MAR 21 1984
Transport Canada / Transports Canada